TRANSFORM DOMAIN STUDY OF CYCLIC AND ABELIAN CODES OVER RESIDUE CLASS INTEGER RINGS

A Thesis Submitted
In Partial fulfilment of the Requirements
for the Degree of
DOCTOR OF PHILOSOPHY

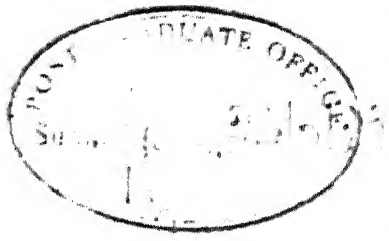
by

B. SUNDAR RAJAN

to the

DEPARTMENT OF ELECTRICAL ENGINEERING
INDIAN INSTITUTE OF TECHNOLOGY, KANPUR

July, 1989



CERTIFICATE

Certified that this work 'TRANSFORM DOMAIN STUDY OF CYCLIC AND ABELIAN CODES OVER RESIDUE CLASS INTEGER RINGS by Mr. B. Sundar Rajan has been carried out under my supervisio and that this has not been submitted elsewhere for a degree.

July, 1989

(M.U.SIDDIQI)
Department of Electrical Engineering
Indian Institute of Technology
Kanpur

ACKNOWLEDGEMENT

I am grateful to my thesis supervisor for his overall guidance throughout the thesis work. I owe a considerable debt to him for reading the first draft very carefully, making numerous corrections and frequently saving me from blunders.

I would like to thank my colleagues, E.G.Rajan, Poonacha, Hari Bhat, Verghese, Madhu and Udaya, for very useful discussions and suggestions. I am particularly thankful to my friend Murali Krishnan for sending me books I required for my work from Syracuse University. But for his prompt help this thesis could have been delayed.

I benefited immensely from many professors of this institute by their teaching and advice. To all of them, I would like to take this opportunity to express my gratitude.

I thank my wife for providing me two very important things, love and time, throughout my work.

TABLE OF CONTENTS

LIST OF SYMBOLS AND NOTATIONS

Z_m	: ring of residue class integers modulo the integer m.
R[X]	: polynomial ring over the ring R.
GF(q)	: Galois field with q elements
$GR(p^k,r)$	: Galois ring $Z_{p^k}[X]/f(X)$, where f(X) is a monic irreducible polynomial of degree r in $Z_{p^k}[X]$
$A \equiv B$	: A is isomorphic to B
$GR^*(p^k,r)$	: Group of units of $GR(p^k,r)$
$A \oplus B$	: direct sum of A and B
$A \otimes B$	: direct product of A and B
R[X]/f(X)	: ring of residue class polynomials modulo the polynomial f(X) belonging to R[X]
a/b	: a divided by b
$a \mid b$	: a divides b
(a,b)	: greatest common divisor of a and b
$a \in R$	: a is an element of the set B
R^n	: the set of ordered n-tuples from the set R
DFT	: discrete Fourier transform
p	: a prime integer
$C_{p,n}(j)$	: conjugacy class containing j corresponding to the integer n and prime p
$\dot{+}$	: addition in mixed radix number system
$\dot{-}$	: subtraction in mixed radix number system
$a > b$	: a is greater than b
$a < b$	: a is less than b
$a \leq b$	: a is less than or equal to b
$a \geq b$	: a is greater than or equal to b

$\|A\|$	: number of elements in the set A
$==>$	: implies
$C^{\perp}$	: Dual code of the code C
Q.E.D.	: end of proof
$A \subset B$	: set A is properly contained in set B

LIST OF TABLES

LIST OF FIGURES

SYNOPSIS

B.Sundar Rajan
Department of Electrical Engineering
Indian Institute of Technology, Kanpur
India

TRANSFORM DOMAIN STUDY OF CYCLIC AND ABELIAN CODES OVER RESIDUE CLASS INTEGER RINGS

Linear block codes for error control have been widely studied over the last four decades under the assumption that the symbols to be transmitted have the structure of a finite field. This assumption restricts the size of the alphabet to a power of a prime number. For arbitrary alphabet size an appropriate mathematical structure to consider is the class of residue class integer rings Z_m. Several authors have investigated linear block codes over Z_m. Like the case of codes over finite fields, most of these studies have considered only the special class of linear cyclic codes over Z_m. Very few results are available for the general class of Abelian codes over Z_m. Studies for the class of linear cyclic codes over Z_m have comprised of: (i) derivation of cyclic codes over Z_m, for m equal to a product of distinct primes, from cyclic codes over finite fields, (ii) derivation of parity check matrices for codes over Z_m analogous to parity check matrices of Hamming and Reed-Solomon codes over finite fields, (iii) construction of BCH codes over Z_{p^k} from BCH codes over p-adic fields, and (iv) BCH codes over Z_m in terms

of generator polynomials.

In this thesis linear cyclic and Abelian error control codes over residue class integer rings Z_m are studied in the transform or frequency domain using discrete Fourier transform (DFT) defined over appropriate extension rings of Z_m. This constitutes a two step generalisation of the well-documented transform domain approach for studying cyclic codes over finite fields. The first step consists of generalising the transform domain approach for cyclic codes over finite fields to cyclic codes over Z_m. When m is a prime number, the results are same as those for cyclic codes over finite fields of prime order. In the second step, the transform domain approach to cyclic codes over Z_m has been generalized to transform domain approach to Abelian codes over Z_m.

Given an alphabet Z_m and code length n, our starting point is the identification of an appropriate extension ring of Z_m, which will support a DFT of length n. For $m = p^k$, the extension ring is the Galois ring, that is, the residue class polynomial ring $Z_{p^k}[X]/\emptyset[X]$, where $\emptyset[X]$ is a monic irreducible polynomial of degree r in $Z_{p^k}[X]$. For arbitrary integer m, the extension ring is a direct sum of Galois rings.

The DFT defines an isomorphism between convolution algebra of n-tuples over Z_m and pointwise product algebra of a subset of the set of n-tuples over the extension ring. This isomorphism is used to obtain transform domain characterization of cyclic codes

over Z_m. It is shown that a cyclic code over Z_m consists of those n-tuples over Z_m whose DFT vectors are constrained to have elements from only particular ideals, both trivial and nontrivial ideals, of the extension ring, in appropriately specified spectral components. This is a generalisation of the result for cyclic codes over finite fields which states that a cyclic code in the transform domain is completely characterised by its spectral zeros in a specified set of spectral components. It may be noted, however, that since nontrivial ideals are absent in finite fields, spectral zeros alone specify a cyclic code over a finite field.

For the case when m is equal to a power of a prime, it is shown that the subset of the set of n-tuples over the extension ring of Z_m, to which the DFT maps the set of all n-tuples over Z_m, is isomorphic to a direct sum of certain subrings of the extension ring. Using this isomorphism, it is argued that every cyclic code of length n over Z_{p^k} consists of the inverse DFT vectors of all n-tuples which contain elements of certain ideals of the subrings of the extension ring, in specified spectral locations. This result is then extended to any arbitrary integer m.

The transform domain identification of cyclic codes over Z_m is particularly simple in the special case when m is equal to a product of distinct primes. For this case it is proved that every cyclic code has an idempotent generator and knowledge of

idempotent elements of Z_m alone is sufficient to identify idempotent generators in the transform domain.

Both Hamming and Lee metric are useful for codes over Z_m depending upon the choice of modulation and decoding schemes. For Hamming metric, it is proved that cyclic codes with elements from nontrivial ideals for spectral components have the same minimum distance as codes with elements from full ring in the same spectral components. In other words, the minimum Hamming distance of cyclic codes over Z_m depends only on zero DFT coefficients. The minimum Lee distance of cyclic codes over Z_m, however, depends on the ideal from which spectral components assume values. In some cases it is observed that, for the same number of codewords, minimum Lee distance of codes with spectral components having values from nontrivial ideals is larger than that of codes with spectral components having values only from trivial ideals.

The transform domain approach to cyclic codes over Z_m is extended to Abelian codes over Z_m. This is achieved by generalising the indexing scheme for codeword components and DFT coefficients. In the case of cyclic codes, it is observed that the indexing elements can be interpreted as elements of a fixed radix number system. For the Abelian case, it is shown that an indexing scheme for codeword and DFT components based on an appropriately chosen mixed-radix number system leads to results similar to those obtained for the cyclic case. The chosen mixed-radix number system depends on the factorisation of the

Abelian group under consideration into direct product of its cyclic subgroups.

Dual code pairs are characterised for both cyclic and Abelian codes over Z_m in terms of spectral components of codewords. This leads to a simple transform domain characterisation of self-dual codes. In particular it is shown that when n and m are relatively prime and $m = p_1^{k_1} p_2^{k_2} \ldots\ldots p_s^{k_s}$, cyclic and Abelian self-dual codes do not exist if any one of k_i, $i = 1,2,\ldots,s$, is odd.

The problem of decoding, with respect to the Hamming metric, is considered for a specific class of cyclic codes over Z_m, viz., t-error correcting BCH codes having 2t consecutive zero spectral components (A BCH code, in general, is defined as a cyclic code with 2t consecutive spectral components having values from the same ideal, including trivial ideals.). In this connection it is proved that the problem of decoding BCH codes over Z_m is equivalent to minimal length shift register synthesis over appropriate Galois rings. This result is the counterpart of the well known equivalence of the decoding problem of BCH codes over a finite field to a minimal length shift register synthesis problem over an appropriate extension of the finite field. For shift register synthesis over Galois rings, an existing algorithm for shift register synthesis over residue class integer rings has been modified to render it applicable for shift register synthesis over any Galois ring.

Finally, some applications of codes over Z_m are discussed. In particular, it is proposed to use the direct sum decomposition of codes over Z_m into codes over Z_{p^k} as a tool for multiplexing information. For certain multiuser communication systems, it is shown that the transform domain approach provides computationally efficient implementation of encoders and decoders for codes over Z_m.

CHAPTER 1

INTRODUCTION

1.1 MOTIVATION

Most of the error correcting codes studies have been over finite fields [1-6]. This means the size of the alphabet consisting of the symbols to be transmitted is assumed to be either a prime number or a power of a prime number. Though this includes the important class of binary alphabet, for certain situations codes defined over alphabets of arbitrary size are essential. Codes for a channel that can transmit more than two levels, multilevel, is practical if the channel is sufficiently quiet, as, for example, the submarine voice cable [7]. In a multilevel transmission system [7] where the number of levels used is not a power of a prime, the alphabet cannot be assumed to have the structure of a finite field. Also in phase modulated channels [1], where the number of distinct phases used is not a power of a prime, finite field structure can not be assumed for the alphabet. In such situations an appropriate mathematical structure to consider is finite commutative ring with identity. The assumption of finite ring structure for alphabet does not put any constraint on the size of the alphabet.

Codes defined over alphabets that are less structured than finite fields may be better suited for certain situations. For example, in computer to computer data transmission the arithmetic of nonprime finite fields is not particularly well suited to computer compared to the arithmetic of residue class integer rings modulo an integer. Whereas the arithmetic of nonprime finite fields is significantly different from integer arithmetic, the arithmetic in residue class integer rings modulo an integer m is same as that of integer arithmetic used in computers with the only difference that integers which give same remainder when divided by m are represented by the remainder in every stage of computation.

Even when the alphabet size is a power of a prime, the symbols can be assumed to constitute other algebraic structures and a natural choice for a general structure, which includes finite field structure as a subclass, is that of a finite commutative ring with identity. Study of codes with finite commutative ring assumption on the alphabet may give better insight into codes over finite field since finite commutative rings include finite field case as a subclass. Also this will provide a general theory of error correcting codes which will include the finite field case as a special case.

There are several classes of finite rings, like integer residue class rings, polynomial residue class rings over finite fields, and polynomial residue class rings over finite rings etc.

Our study has been restricted mainly to integer residue class rings Z_m. Specifically, in this thesis we study linear block codes for error control over residue class integer ring Z_m in the transform domain using discrete Fourier transform over an extension ring of Z_m.

1.2 HISTORICAL BACKGROUND

Several authors have studied codes over Z_m from different points of view. Compared to the literature for codes over finite fields, the literature available for codes over Z_m is very scant. In this section we briefly review the literature available on codes over Z_m.

To our knowledge, the first paper on codes over Z_m appears to be by Blake [8] in which he has obtained cyclic codes over Z_m for the case when m is a product of distinct primes from codes over finite fields. Specifically, he constructs a linear cyclic code of length n over Z_m, $m=p_1p_2...p_s$, which has minimum Hamming distance d, from linear cyclic codes of length n over $GF(p_i)$ with minimum Hamming distance d_i, $i=1,2,...s$, and shows that d is equal to the minimum of d_i, $i=1,2,...s$. In a subsequent paper [9] he has defined, for $m=p^k$, natural analogs to Hamming, Reed-Solomon codes. An attempt is made to obtain BCH codes over Z_m, and some ring theoretic problems one encounters when working over Z_m are discussed.

Spiegel [10,11] has constructed (i) cyclic codes over Z_m, where $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, from codes over Z_{p^k} and (ii) BCH codes over Z_{p^k} from BCH codes over p-adic fields and their residue class fields.

In terms of generator polynomials cyclic and BCH codes over Z_m, for arbitrary value of m, have been obtained by Prithi Shankar [12]. It is shown that in Galois rings, extension rings of Z_{p^k}, the polynomial (x^n-1) factors uniquely and this is the key idea that helps in describing cyclic codes over Z_m in a manner that is very similar to cyclic codes over finite fields.

Very few results are available for the general class of Abelian codes over Z_m [13]. In [13] the factorisation of Abelian codes over Z_m, corresponding to the factorisation of m into product of distinct primes and factorisation of Abelian group into product of cyclic groups, are considered.

Our approach is along the lines of Blahut, who has studied codes over finite field in the transform domain using discrete Fourier transform defined over finite fields [14,15], and is a generalisation of Blahut's approach for codes over prime fields to codes over integer residue class rings. Historically, the idea of using discrete Fourier transform for codewords over finite fields appeared in the literature much earlier than Blahut's work in the form of Mattson-Solomon polynomials [16].

Discrete Fourier transforms over different finite rings are used widely in the area of Digital signal processing [17-23]. However, in the area of error correcting codes it does not appear to have been used as widely. In this thesis, our main tool is discrete Fourier transform defined over an appropriate extension ring of Z_m. Our starting point, for the purpose of studying codes over Z_m, is the identification of an appropriate extension ring of Z_m, called Galois ring, in which discrete Fourier transform is defined. Codes are characterised in terms of transform coefficients, called DFT coefficients or spectral components, taking values from ideals, both trivial and nontrivial ideals, of Galois rings.

1.3 OUTLINE OF CHAPTERS

Chapter 2 deals with the mathematical background required for the transform domain study of codes over Z_m. This chapter deals mainly with Galois rings and related concepts like discrete Fourier transform over them and conjugacy classes. General properties of Galois rings that are of interest for our study are listed with illustrated examples. The necessary and sufficient conditions for a Galois ring to support a DFT of given length is given. The notion of conjugacy symmetry property of DFT over Galois rings is explained. This leads to the notion of conjugacy classes whose structure is discussed in detail. Modules over finite rings and Group rings are discussed briefly.

In Chapter 3, linear and cyclic codes over Z_m are defined. The nature of problems that arise due to the presence of zero divisors in Z_m, in contrast to the case of finite fields, is discussed. This leads to the notion of word-length of a linear code over Z_m, which is the counterpart of the notion of dimension in the case of linear codes over finite fields. Various possible approaches one could take for studying cyclic codes, viz., polynomial theoretic approach, Group algebra approach and transform domain approach are briefly explained. In the next chapter cyclic codes over Z_m are studied in the transform domain.

Transform domain characterisation of cyclic codes over Z_m is obtained in Chapter 4. Three different cases are considered (i) m is a power of a prime, p^k, (ii) m is any arbitrary integer $p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, (iii) m is a product of distinct primes $p_1 p_2 \ldots p_s$. For the case $m = p^k$, it is shown that, for length n cyclic codes, the extension ring that supports a DFT is the Galois ring $GR(p^k,r)$, where r is the least integer such that n divides (p^r-1). It is proved that the transform vectors of all n-tuples over Z_{p^k} is isomorphic to the direct sum of certain subrings of the Galois ring $GR(p^k,r)$, given by $\bigoplus_{i=1}^{t} GR(p^k,r_i)$, where t is the number of conjugacy classes and r_i, i=1,2,..,t, are the exponents of the conjugacy classes. This direct sum of subrings is denoted by R_T. Using this isomorphism, a cyclic code of length n over Z_{p^k} is defined as the set of n-tuples over Z_{p^k} which consists of the inverse DFT vectors of all vectors of R_T, whose specified spectral components take values from specified ideals, including

nontrivial ideals, of $GR(p^k, r_i)$, i=1,2,..,t. The minimum Hamming distance of these codes is shown to depend only on zero spectral components and not on the ideals from which nonzero spectral components are taken. An expression for word-length is obtained in terms of exponents of the conjugacy classes and ideals occupying those conjugacy classes. These results are then extended to arbitrary value of m in the next subsection. In the special case of $m = p_1 p_2 \ldots p_s$, it is shown that every cyclic code over Z_m has an idempotent generator which can be specified in the transform domain in terms of idempotent elements of Z_m. In the last section of this chapter BCH codes over Z_m are discussed. BCH codes are defined as the cyclic codes with 2t consecutive spectral components taking values from the same specified ideal, including nontrivial ideals.

A generalisation of cyclic codes over Z_m, called Abelian codes, are discussed in Chapter 5. It is shown that the suitable indexing scheme for codewords and their DFT coefficients, for transform domain study of these codes is the mixed radix number systems in contrast to the fixed radix number systems for cyclic codes. A generalised DFT suitable for Abelian codes is defined. This naturally leads to the notion of conjugacy classes and conjugacy symmetry property in a mixed radix number system. Using this generalised DFT, transform domain characterisation of Abelian codes and results similar to those obtained for the cyclic codes over Z_m are obtained, for Abelian codes over Z_m.

Chapter 6 deals with dual codes of cyclic and Abelian codes over Z_m. Dual code of a given linear code over Z_m is defined. For both cyclic and Abelian codes over Z_m, dual code pairs are characterised in terms of spectral components of codewords. A simple transform domain characterisation of cyclic and Abelian self-dual codes is obtained. It is proved that when n and m are relatively prime and $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, cyclic and Abelian self-dual codes do not exist, if any one of k_i, $i=1,2,\ldots,s$, is odd.

In Chapter 7, the problem of decoding is considered for a specific class of BCH codes over Z_m, viz., BCH codes with consecutive zero spectral components. The decoding is for the Hamming metric. It is shown that the decoding problem of these BCH codes is equivalent to the shift register synthesis problem over Galois rings. An algorithm for shift register synthesis over Galois rings is obtained by modifying slightly the algorithm of Reeds-Sloane, which is for shift register synthesis over Z_m.

In Chapter 8, applications of codes over Z_m are discussed. It is shown that in certain multiuser communication systems, codes over Z_m can be used to implement computationally efficient encoders and decoders. Also it is proposed to use codes over Z_m as a tool for multiplexing information.

Chapter 9, the concluding chapter, contains a summary of results obtained in this thesis. Also few suggestions regarding further research in various directions are given.

CHAPTER 2

MATHEMATICAL BACKGROUND

Essentially this chapter deals with the mathematical tools required for transform domain study of codes over Z_m.

Familiarity with algebraic structures like groups, rings and vector spaces, their properties and important results concerning them, along with notions like homomorphism and isomorphism are assumed. These can be found in any well known text book on algebra and coding theory. Only those results and concepts which will be used often and not found in well known text books are collected in this chapter.

In the case of codes over finite fields, the notion of algebraic extension of a field and the structure of extension fields play important roles. Similarly, for the study of codes over Z_m, clear knowledge of notion of ring extensions, especially extension rings of Z_m, is important. This plays a central role throughout the thesis. This chapter deals with the properties and structure of Galois rings with related concepts like discrete Fourier transform (DFT) defined over them and conjugacy classes, which are the main tools for our study in the transform domain. A detailed treatment of Galois rings can be found in [24].

2.1 GALOIS RINGS

Definition: Let p^k be a power of a prime number. Galois rings are residue class polynomial rings $Z_{p^k}[X]/\emptyset(X)$, denoted by $GR(p^k,r)$, where $Z_{p^k}[X]$ is the ring of polynomials over Z_{p^k} and $\emptyset(X)$ is a monic irreducible polynomial of degree r belonging to $Z_{p^k}[X]$.

It is easy to see that $GR(p^k,1)$ is isomorphic to Z_{p^k} and $GR(p,r)$ is isomorphic to $GF(p^r)$. Properties and results of Galois rings that are of interest to us are listed below with examples.

Fact 2.1: If $\emptyset_1[X]$ and $\emptyset_2[X]$ are monic irreducible polynomials of degree r in $Z_{p^k}[X]$ then $Z_{p^k}[X]/\emptyset_1[X] \equiv Z_{p^k}[X]/\emptyset_2[X]$. This justifies the notation $GR(p^k,r)$ [24].

Fact 2.2: Every ideal in $GR(p^k,r)$ is generated by p^i, of the form $\langle p^i \rangle = p^i GR(p^k,r)$ for $0 \leq i \leq k$. The maximal ideal is $pGR(p^k,r)$. i.e., $GR(p^k,r)$ is a principal ideal ring as well as a local ring [24].

Fact 2.3: Every non-zero element θ in $GR(p^k,r)$ can be written as up^t, where u is a unit, $0 \leq t \leq k-1$, and in this representation the integer t is unique and u is unique modulo p^{k-t} [25].

Fact 2.4: [25, Theorem XVI.9] If $GR^*(p^k,r)$ denotes the group of units of $GR(p^k,r)$ then $GR^*(p^k,r) \equiv G_1 \times G_2$ (direct product of groups) where

(a) G_1 is the cyclic group of order p^r-1 and this is the only cyclic subgroup of $GR^*(p^k,r)$ of order relatively prime to p.

(b) G_2 is an abelian group of order $p^{(k-1)r}$.

Fact 2.5: [25, Proposition 2] The group of automorphisms of $GR(p^k,r)$ is a cyclic group of order r.

Fact 2.6: [12, Theorem 3] In general, factorization in rings with zero divisors is not unique. But when (n,p) = 1, the polynomial (X^n-1) factors uniquely in $GR^*(p^k,r)$.

Fact 2.7: [24, Theorem XVI.7] Every subring of $GR(p^k,r)$ is a Galois ring of the form $GR(p^k,d)$, where d divides r. Conversely if d divides r then $GR(p^k,r)$ contains a unique subring isomorphic to $GR(p^k,d)$.

Example 2.1: Let p=2, k=2 and r=2. Monic irreducible polynomials of degree 2 in $Z_4[X]$ are listed below.

$\emptyset_1(X) = X^2+X+1$, $\emptyset_2(X) = X^2+X+3$, $\emptyset_3(X) = X^2+3X+1$, and $\emptyset_4(X) = X^2+3X+3$.

Any one of the above polynomials for the choice of $\emptyset(X)$ in $Z_4[X]/\emptyset(X)$ will result in $GR(p^k,r)$. Ideals of GR(4,2) are

$I_1 = \{ 0 \}$

$I_2 = \{ 0, 2, 2X, 2+2X \} \equiv 2^1\ GR(4,2)$ and

$I_3 = \{ 0, 1, 2, 3, X, X+1, X+2, X+3, 2X, 2X+1, 2X+2, 2X+3, 3X, 3X+1, 3X+2, 3X+3 \}$

$\equiv 2^0\ GR(4,2) \equiv GR(4,2)$.

The maximal ideal is I_2 and it is clear that GR(4,2) is a local ring. Generator polynomial for I_2 is 2X and for I_3 it is X. Subrings of GR(4,2) are

SR_1 = { 0 }

SR_2 = { 0, 1, 2, 3 } $\equiv$ GR(4,1) and

SR_3 = GR(4,2).

The representation of nonzero elements of GR(4,2) as in Fact 2.3 is as follows.

θ	t	u	u(mod $2^{(2-t)}$)	θ	t	u	u(mod $2^{(2-t)}$)
1	0	1	1	1+2X	1	1+2X	1+2X
2	1	1 or 3	1	2+2X	1	1+X or 3+3X	1+X
3	0	3	3	3+2X	0	3+2X	3+2X
X	0	X	X	3X	0	3X	3X
1+X	0	1+X	1+X	1+3X	0	1+3X	1+3X
2+X	0	2+X	2+x	2+3X	0	2+3X	2+3X
3+X	0	3+X	3+X	3+3X	0	3+3X	3+3X
2X	1	X or 3X	X				

The group of units is

$GR^*(4,2)$ = { 1, 3, X, 1+X, 2+X, 3+X, 1+2X, 3+2X, 3X, 1+3X, 2+3X, 3+3X }

and G_1 is { X, 3+3X, 1 }. The generator of the automorphism group of GR(4,2) is σ: X $\longrightarrow$ 3X+3. Clearly $\sigma^2(X) = 3(3X+3)+3 = X$. i.e., the automorphism group is the cyclic group of order 2. Also

it is clear that (x^3-1) factors uniquely as $(x-1)(x-\alpha)(x-\alpha^2)$ where $\alpha = X$ and $\alpha^2 = 3+3X$.

Example 2.2: Let m=8 and r=2.

$\emptyset(X) = X^2+X+1$ is an irreducible polynomial of degree 2 in $Z_8[X]$.

$GR(8,2) = Z_8[X]/(X^2+X+1)$.

Ideals of GR(8,2) are

$I_1 = \{ 0 \}$

$I_2 = \{ 0, 4, 4X, 4+4X \} \equiv 2^2GR(8,2)$

$I_3 = \{ 0, 2, 6+2X, 6+6X, 2+4X, 4+4X, 2X, 4, 6X, 2+6X, 6+4X, 2+2X, 6, 4+6X, 4X, 4+2X \}$

$\equiv 2\ GR(8,2)$ and

$I_4 = GR(8,2)$.

Subrings of GR(8,2) are

$SR_1 = \{ 0 \}$

$SR_2 = \{ 0, 1, 2, 3, 4, 5, 6, 7 \} \equiv GR(8,1)$ and

$SR_3 = GR(8,2)$.

The only cyclic subgroup of order relatively prime to 8 in $GR^*(8,2)$, i.e., G_1 is $\{ 1, X, 7+7X \}$.

The generator of the automorphism group is σ: $X \longrightarrow 7+7X$.

Example 2.3: Let m=9 and r=2.

$\emptyset(X) = X^2+X+2$ is an irreducible polynomial of degree 2 in $Z_8[X]$.

$GR(9,2) = Z_8[X]/(X^2+X+2)$.

Ideals of GR(9,2) are

I_1 = (0)

I_2 = (0, 3, 3+6X, 6, 6+6X, 6+3X, 6X, 3X, 3+3X)

≡ 3^1GR(9,2) and

I_3 = GR(9,2).

Subrings of GR(9,2) are

SR_1 = (0)

SR_2 = (0, 1, 2, 3, 4, 5, 6, 7, 8) ≡ GR(9,1) and

SR_3 = GR(9,2).

Fact 2.8: [24, Theorem VI.2] An arbitrary finite commutative ring R with identity is isomorphic to a direct sum of local rings. This decomposition into local rings is unique upto the order of summands.

Example 2.4:

(a) Let $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$. Then

$$Z_m \equiv Z_{p_1^{k_1}} \oplus Z_{p_2^{k_2}} \oplus \ldots \oplus Z_{p_s^{k_s}}.$$

This isomorphism is the well known Chinese remainder theorem given by the following mapping

$\emptyset(X) = (x_1, x_2, \ldots, x_s)$ for $X \in Z_m$ and $x_i \in Z_{p_i^{k_i}}$ where x_i is given by $x_i = X \pmod{p_i^{k_i}}$.

(b) Let $f(X) = f_1^{t_1}(X) f_2^{t_2}(X) \ldots f_s^{t_s}(X)$, where $f_i(X)$, $i=1,2,\ldots,s$, is irreducible over GF(q)[X]. Then

$$GF(q)[X]/f(X) \equiv GF(q)[X]/f_1^{t_1}(X) \oplus \ldots\ldots \oplus GF(q)[X]/f_s^{t_s}(X).$$

(c) $$Z_m[X]/(X^n-1) \equiv Z_{p_1^{k_1}}[X]/(X^n-1) \oplus \ldots. \oplus Z_{p_s^{k_s}}[X]/(X^n-1).$$

In general, if $f(X) = f_1(X)\, f_2(X) \ldots. f_s(X)$, then

$$Z_m[X]/f(X) \equiv Z_m[X]/f_1(X) \oplus \ldots. \oplus Z_m[X]/f_s(X).$$

For $m = p_1^{k_1} p_2^{k_2} \ldots p_t^{k_t}$ and $f(X) = f_1(X) f_2(X) \ldots. f_s(X)$ we have

$$Z_m[X] \equiv \bigoplus_{i=i}^{t} \bigoplus_{j=1}^{s} Z_{p_i^{k_i}}[X]/f_j(X)$$

2.2 DISCRETE FOURIER TRANSFORM (DFT) OVER FINITE RINGS

A finite commutative ring with identity, denoted by R, is said to support a discrete Fourier transform (DFT) of length n if there exists a transform of the form

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i, \qquad j=0,1,\ldots,(n-1),$$

where a_i, $A_j \in R$, and α is a unit of order n in the group of units of R and n is invertible in R. The element α is called the transform factor (TF) of the DFT.

This DFT defines an isomorphism between convolution algebra $R[X]/(X^n-1)$ and pointwise product algebra of n-tuples of R, denoted by R^n. In other words, if $(A_0,A_1,\ldots,A_{n-1})$ and $(B_0,B_1,\ldots,B_{n-1})$ are the transform vectors of $(a_0,a_1,\ldots,a_{n-1})$ and $(b_0,b_1,\ldots,b_{n-1})$ then the cyclic convolution

$$c_k = \sum_{i=0}^{n-1} a_i \, b_{(k-i) \bmod n},$$

$k=0,1,\ldots,n-1$, has the transform vector $(C_0,C_1,\ldots,C_{n-1})$ where $C_k = A_kB_k$, $k=0,1,\ldots,(n-1)$. This property is known as convolution property of the DFT.

Fact 2.9: [22, Theorem 1] If R is a direct sum of local rings $R_1,R_2,\ldots,R_t$ then R supports a DFT of length n iff R_i, $i=0,1,\ldots,t$, supports a DFT of length n.

Fact 2.10: [22, Theorem 3] Let $R \equiv R_1 \oplus R_2 \oplus \ldots \oplus R_t$ where R_i, $i=1,2,\ldots,t$, is a local ring. Then R supports a DFT of length n iff

(i) R_i contains an element α_i of order n.

(ii) n is invertible in R_i. i.e., n is a unit in R_i.

2.2.1 DFT over Galois rings

For a Galois ring $GR(p^k,r)$ to support a DFT of length n (see Fact 2.10) it is required that n and p must be relatively prime, i.e., $(n,p) = 1$, and n should divide p^r-1, since then only

an element α of order n can exist in $GR(p^k,r)$ (see Fact 2.4). Now using Fact 2.10, it is clear that $\bigotimes_{i=1}^{s} GR(p_i^{k_i},r)$ can support a DFT of length n iff the following conditions are satisfied.

(i) $(n,p_i) = 1$ for $i=1,2,\ldots,s$.

(ii) $n \mid \gcd((p_1^r-1),(p_2^r-1),\ldots,(p_s^r-1))$

Hence for our purpose of studying codes over Z_m using DFT the choices for the length of the code get restricted to those integers n which are relatively prime to m. Therefore throughout the thesis it is assumed that the length of the code, denoted by n, is relatively prime to m.

In the familiar case of DFT over the complex field C, if $(A_0,A_1,\ldots,A_{n-1})$ is the transform vector of $(a_0,a_1,\ldots,a_{n-1})$ defined by

$$A_j = \sum_{i=0}^{n-1} \exp(2\pi i j/n)\, a_i$$

where a_i's $\in$ R, where R denotes real number field, and A_i's $\in$ C, it is well known that A_j is the complex conjugate of A_{n-j}. A similar property holds in the case of DFT over finite fields also. Let $GF(q^m)$ be the extension field of GF(q) such that m is the least integer such that n divides q^m-1, where n is the length of the vector. DFT is defined by

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij}\, a_i$$

where α is an element of order n in $GF(q^m)$. If $(a_0,a_1,\ldots,a_{n-1})$,

a n-tuple over GF(q), has the transform vector $(A_0,A_1,\ldots,A_{n-1})$ which is a n-tuple over $GF(q^m)$ it is known [14,15] that the DFT coefficients satisfy the relation

$$A_{(qj) \bmod n} = A_j^q.$$

In other words the coefficients of $(A_j, A_{qj}, A_{q^2 j}, \ldots, A_{q^{e-1} j})$ are related. The set $(j, qj, q^2 j, \ldots, q^{e-1} j)$ is called the conjugacy class containing j and the above relation is called conjugacy constraint. Only n-tuples over $GF(q^m)$ which satisfy the conjugacy constraint will have inverse DFT coefficients belonging to the ground field. In the case of complex field only n-tuples over C which satisfy the relation $A_j = A^*_{n-j}$ will be the DFT of some n-tuple over the real field. It is interesting to note that in both cases the conjugacy constraint defines an automorphism of the field in which DFT is defined. Explicitly, the mapping given by $\sigma : (a+ib) \longrightarrow (a-ib)$ defines an automorphism of C and the mapping $\sigma: \alpha \longrightarrow \alpha^q$, defines an automorphism in $GF(q^m)$.

A similar property, known as conjugate symmetry property, holds in the case of DFT over Galois rings. Let $(a_0,a_1,\ldots,a_{n-1})$ be an n-tuple over Z_{p^k} and $(A_0,A_1,\ldots,A_{n-1}) \in GR^n(p^k,r)$ be its transform vector, where $GR(p^k,r)$ is the extension ring of Z_{p^k} which supports the DFT. We have

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i$$

where α is an element of order n in $GR^*(p^k,r)$. The automorphism group of $GR(p^k,r)$ is a cyclic group of order r and the generator

automorphism is $\sigma(\alpha) = \alpha^p$. The conjugacy constraint in this case is given by

$$A_{pj} = \sigma(A_j) \quad \text{for all } j.$$

All the n-tuples of $GR(p^k,r)$ which are DFT vectors of some n-tuple over Z_{p^k} satisfy this condition. This property is called the conjugate symmetry property of DFT over Galois rings.

Example 2.5 Let n=3 and m=4. From Example 2.1, we can choose $\alpha = x$ and the transform matrix is

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 3x+3 & x \\ 1 & x & 3x+3 \end{bmatrix}$$

Transform vectors, (A_0,A_1,A_2), of all 3-tuples over Z_4, (a_0,a_1,a_2), are listed in Table 2.1. An element a+bx of GR(4,2) is denoted simply by ab. The generator of the automorphism group is σ, given by $\sigma(x) = 3+3x$.

Table 2.1 Listing of 3-tuples over Z_4 and their transform vectors corresponding to Example 2.5

codeword (a_0,a_1,a_2)	spectrum (A_0,A_1,A_2)	codeword (a_0,a_1,a_2)	spectrum (A_0,A_1,A_2)
0 0 0	00 00 00	2 0 0	20 20 20
0 0 1	10 01 33	2 0 1	30 21 13
0 0 2	20 22 02	2 0 2	00 02 22
0 0 3	30 03 11	2 0 3	10 23 31
0 1 0	10 33 01	2 1 0	30 13 21
0 1 1	20 30 30	2 1 1	00 10 10
0 1 2	30 31 23	2 1 2	10 11 03
0 1 3	00 12 32	2 1 3	20 32 12
0 2 0	20 20 22	2 2 0	00 22 02
0 2 1	30 23 31	2 2 1	10 03 11
0 2 2	00 20 20	2 2 2	20 00 00
0 2 3	10 21 13	2 2 3	30 01 33
0 3 0	30 11 03	2 3 0	10 31 23
0 3 1	00 32 12	2 3 1	20 12 32
0 3 2	10 31 23	2 3 2	30 33 01
0 3 3	20 10 10	2 3 3	00 30 30
1 0 0	10 10 10	3 0 0	30 30 30
1 0 1	20 03 11	3 0 1	00 23 31
1 0 2	30 12 32	3 0 2	10 32 12
1 0 3	00 21 13	3 0 3	20 01 33
1 1 0	20 11 03	3 1 0	00 31 23
1 1 1	30 00 00	3 1 1	10 20 20
1 1 2	00 33 01	3 1 2	20 13 21
1 1 3	10 22 02	3 1 3	30 02 22
1 2 0	30 32 12	3 2 0	10 12 32
1 2 1	00 01 33	3 2 1	20 21 13
1 2 2	10 30 30	3 2 2	30 10 10
1 2 3	20 23 31	3 2 3	00 03 11
1 3 0	00 13 21	3 3 0	20 33 01
1 3 1	10 02 22	3 3 1	30 22 02
1 3 2	20 31 23	3 3 2	00 11 03
1 3 3	30 20 20	3 3 3	10 00 00

2.2.2 Conjugacy class structure

Definition 2.1: Given a positive integer n and a prime p relatively prime to n, the conjugacy class containing j, ($0 \leq j \leq n$), denoted by $C_{p,n}(j)$ is the set

$$\{ j, pj, p^2j, \ldots, p^{(e-1)}j \}$$

where e is the least integer such that $p^e j = j \pmod{n}$. Such an integer exists because of relative primality of n and p. The integer e is called the exponent of the conjugacy class $C_{p,n}(j)$ and is denoted by $\exp(C_{p,n}(j))$.

It is clear that the cardinality of $C_{p,n}(j)$ is equal to $\exp(C_{p,n}(j))$. The conjugacy class structure for a given n and p^k, which is a partition of $\{ 0, 1, 2, \ldots, (n-1) \}$ depends only on n and the prime p, and not on k. Moreover, the conjugacy class structure implies a good deal of structure of the codes, which is discussed in the subsequent chapters. For these reasons the structure of conjugacy class is discussed in detail in this section.

For two relatively prime integers a and b, the least integer r such that $a^r = 1 \pmod{b}$ is called the exponent of a mod b, denoted by $\exp_b(a)$.

The following results follow from the definition of conjugacy classes:

(1) (a) If (j,n) = 1, then $\exp(C_{p,n}(j)) = \exp_n(p)$.

(b) If (j,n) = d, then $\exp(C_{p,n}(j)) = \exp_q(p)$ where $q = (n/d)$.

(2) If $p_1 = p_2 \pmod n$, then $C_{p_1,n}(j) = C_{p_2,n}(j)$, $j=0,1,..,(n-1)$.

(3) If $p = 1 \pmod n$, then the conjugacy classes are

$$C_{p,n}(j) = \{\ j\ \} \quad \text{for all } j.$$

Example 2.6: (1) Let n=8 and p=7. The conjugacy classes are { 0 }, { 1,7 }, { 2,6 } and { 4 }.

(2) Let n=7 and p=13. The conjugacy classes are {0}, {1,6}, {2,5} and {3,4}.

Theorem 2.1: For a given n, the number of different sets of conjugacy classes for different values of p is atmost Ø(n) where Ø(n) is the Euler's Phi function.

Proof: For a fixed prime p let $p \pmod n = a$, $0 \le a \le (n-1)$ and let $d = \gcd(n,a)$. Then

$$\begin{aligned} p \pmod n = a &\Longrightarrow p = kn+a \\ &\Longrightarrow p = d(k(n/d)+(a/d)) \\ &\Longrightarrow d \mid p \\ &\Longrightarrow d = 1 \text{ since } (n,p) = 1 \\ &\Longrightarrow (n,a) = 1. \end{aligned}$$

Since two primes p_1 and p_2 with $p_1 = p_2 \pmod n$ have identical conjugacy classes, it follows that there can be at most Ø(n) non-

identical conjugacy class structure for different values of p.

Q.E.D.

Example 2.7: Let n=5. For different possible primes the conjugacy class structure is shown below:

(a) $p = 1 \pmod 5$ { 0 }, { 1 }, { 2 }, { 3 }, { 4 }

(b) $p = 2 \pmod 5$ { 0 }, { 1,2,3,4 }

(c) $p = 3 \pmod 5$ { 0 }, { 1,2,3,4 }

(d) $p = 4 \pmod 5$ { 0 }, { 1,4 }, { 2,3 }

In the above example the conjugacy class structures are same for n=5, $p_1 = 2 \pmod 5$ and n=5, $p_2 = 3 \pmod 5$ though $p_1 \not\equiv p_2$ modulo 5. In Chapter 4, a theorem is given which characterises primes p_1 and p_2 ($p_1 \not\equiv p_2 \pmod n$) which have identical conjugacy class structure for a given n.

Theorem 2.2: Given a prime p and an integer n, the exponent of any conjugacy class divides r, where $\exp_n(p) = r$.

Proof: Since $r = \exp_n(p)$, a least integer r can be chosen such that $p^r = 1 \pmod n$. For $1 \leq j < n$, let $p^e j = j \pmod n$, where e is the least integer satisfying this congruence. Now $e \leq r$, since for r also the congruence $p^r j = j \pmod n$ holds. Let $r = ae+b$ where $0 \leq b < e$. We have

$$p^r j = j \pmod n$$

$$p^{ae+b} j = j \pmod n$$

$$p^b j = j \pmod n \quad \text{since } p^e j = j \pmod n.$$

But e is the least integer satisfying the above congruence. Hence b = 0. i.e, e divides r. Q.E.D.

Theorem 2.3: Given a prime p and an integer n the number of conjugacy classes, denoted by t, is given by

$$t = \sum_{d|n} \frac{\phi(d)}{\exp_q(d)}$$

where q = n/d [26].

2.3 MODULES OVER FINITE RINGS

The set of n-tuples over a finite field GF(q) form a vector space. Codes over GF(q) are studied using the vector space structure. For example a subspace of the vector space is a linear code and a linear cyclic code is a subspace with the property that every cyclic shift of components of a vector in it is also a vector belonging to it. The dimension of a linear code is the dimension of the subspace. In our case of codes over Z_m the set of n-tuples over Z_m have a structure called module.

Definition 2.2: An abelian group M is said to form a module over a ring R if the following conditions are satisfied.

For all r,s $\in$ R and m,n $\in$ M,

(a) r(m+n) = rm+rn

(b) rs(m) = r(sm)

(c) $(r+s)m = rm+sm$

(d) $1m = m$, where 1 is the multiplicative identity in R.

It is called a R-module M.

Some examples of modules are (i) If R is a field, then a vector space over R is a module, (ii) Any infinite abelian group can be considered a Z-module, where Z denotes the ring of integers, (iii) Any ring R is a module over itself with the scalar multiplication being the multiplication of the ring itself. It is clear that the module structure includes infinite abelian groups, rings and vector spaces as particular cases.

If N is an abelian subgroup of a R-module M and whenever r is in R and n is in N then rn is in N, then N is called a R-submodule of M. A subset S of M is said to be linearly independent if whenever $\sum_{s \in S} a_s s = 0$ then $a_s = 0$ for all s in S. A subset S of M is said to be a basis of M if S generates M and S is linearly independent. A free module is one which has a basis. A module M is called simple when its only submodules are 0 and M. It is called semi-simple if it is a direct sum of a family of simple modules or equivalently it is generated by a family of simple submodules.

It is easy to verify that the set of all ordered n-tuples from Z_m form a module over Z_m, Z_m being considered as a ring.

2.4 GROUP RINGS

Let G denote a finite multiplicative group and R a ring. Let R[G] denote the set of formal sums $\sum_{g\in G} r_g\, g$ where $r \in R$. Let us define in R[G] addition, scalar multiplication and multiplication respectively as follows:

$$\sum_{g\in G} r_g\, g + \sum_{g\in G} s_g\, g = \sum_{g\in G} (r_g+s_g)\, g \qquad (2.4.1)$$

$$r\Big(\sum_{g\in G} r_g\, g\Big) = \sum_{g\in G} (rr_g)\, g \qquad (2.4.2)$$

$$\Big(\sum_{g\in G} r_g\, g\Big)\Big(\sum_{h\in G} s_h\, h\Big) = \sum_{k\in G} t_k\, k \quad \text{where} \quad t_k = \sum_{gh=k} r_g s_h. \qquad (2.4.3)$$

Note that R[G] is an R-module with addition and scalar multiplication (2.4.2). It is a free module generated by the set of elements of G. With addition and multiplication (2.4.3), R[G] is a ring called Group ring of G over R. With all the three operations R[G] is an algebra called Group algebra over R.

If R is a field F, then F[G] is called group algebra over F, denoted by FG. Cyclic codes over GF(q) can be interpreted as ideals in the group algebra GF(q)[C] where C is a cyclic group of appropriate order [6]. Similarly Abelian codes are ideals of the group algebra GF(q)[A] where A is an abelian group [27].

The following result will be of use in subsequent chapters.

Theorem 2.4: [28] The group ring R[G] is semi-simple if and only if

(a) R is semi-simple

(b) The order of G is a unit in R.

CHAPTER 3

CODES OVER Z_m

Basic notions concerning codes over Z_m are discussed in this chapter. Linear codes and cyclic codes over Z_m are defined. This chapter essentially deals with the nature of problems that arise due to the difference in the algebraic structure between finite commutative rings with identity and finite fields. Various approaches one could take to study cyclic codes viz., polynomial theoretic approach, group algebra approach and transform domain approach are briefly explained.

3.1 LINEAR CODES OVER Z_m

Definition 3.1: Let Z_m^n denote the module of the set of n-tuples over Z_m. A linear code of length n over Z_m is a submodule of Z_m^n.

Let $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ be the prime power factorisation of m. By the Chinese remainder theorem we have

$$Z_m \equiv Z_{p_1^{k_1}} \oplus Z_{p_2^{k_2}} \oplus \ldots\ldots \oplus Z_{p_s^{k_s}}.$$

It follows from the above isomorphism that

$$Z_m^n \equiv Z_{p_1^{k_1}}^n \oplus Z_{p_2^{k_2}}^n \oplus \cdots \oplus Z_{p_s^{k_s}}^n$$

and hence any linear code over Z_m is isomorphic to a direct sum of linear codes over $Z_{p_i^{k_i}}$, i=1,2,...,s. Hence throughout the chapter it is assumed that $m = p^k$.

The above isomorphism assigns to a set of n-tuples, one each from $Z_{p_i^{k_i}}$, i=1,2,...,s, a unique n-tuple over Z_m. This isomorphism can therefore be used in a multiuser communication system where k sources are encoded, each source's symbols from one of $Z_{p_i^{k_i}}$, and the encoded messages are to be sent through a single wideband channel. Instead of sending all the k encoded messages one can transmit the corresponding n-tuple over Z_m. This aspect has been discussed in Chapter 8.

Z_{p^k} is a local ring with the maximal ideal generated by p and every non-trivial ideal is generated by p^j for some j=1,2,...,k-1. The order of $Z_{p^k}^n$ is equal to p^{kn} and the order of any submodule of $Z_{p^k}^n$ divides p^{kn}. Hence the order of a linear code is of the form p^μ where $0 \leq \mu \leq kn$.

Definition 3.2: Let L be a linear code over Z_{p^k} of length n and its order be p^μ for some μ, $0 \leq \mu \leq kn$. μ is defined as the word-length of the code L.

In the case of codes over GF(p^m) where p is a prime, a linear code which is a subspace of $GF^n(p^m)$ has order p^s where s is a multiple of m. If s = km, then the dimension of the code, same as the dimension of it as the subspace, is k and it is equal to the number of information symbols (message block length) in a codeword. In the case of modules, the notion analogous to dimension in vector space is the notion of rank. In our case of linear code over Z_{p^k}, rank of a submodule does not have this interpretation in terms of message block length. An attempt to interpret word-length in terms of message block length leads to an interesting situation which involves the number of information sources itself. Let us consider few concrete cases of linear codes over Z_4 of length 3. The listing of all the codewords of four codes L1,L2,L3 and L4 is given in Table 3.1.

The word-lengths of the codes L1,L2,L3 and L4 respectively are 3,4,4 and 5. For the message block lengths from Z_4 to be 1,2 or 3, the corresponding code should have 4,16 or 64 codewords respectively. Codes L2 and L3 have 16 codewords and hence two information symbols. What is the message block lengths in the case of codes L1 and L4?. If it is assumed that the message source is one with alphabet size four, then codes L1 and L4, cannot be used as a code. It is suitable as a code if more than one source with different alphabet size are assumed to be coded simultaneously using a single code. For example code L1 can be used in a situation where there are two sources $S_{1,1}$ and $S_{1,2}$ of alphabet size 2 and 4 respectively as shown in Fig 3.1(a). In

Table 3.1 Listing of four codes over Z_4.

Code L1: { (0 0 0), (0 0 2), (2 0 0), (2 0 2), (0 2 0), (0 2 2),
(2 2 0), (2 2 2) }
Number of codewords is 8.

Code L2: { (0 0 0), (1 1 1), (0 0 2), (1 1 3), (2 0 0), (3 1 1),
(2 0 2), (3 1 3), (0 2 0), (1 3 1), (0 2 2), (1 3 3),
(2 2 0), (3 3 1), (2 2 2), (3 3 3) }
Number of codewords is 16.

Code L3: { (0 0 0), (1 2 1), (0 1 3), (3 1 0), (0 3 1), (3 2 3),
(2 2 0), (2 0 2), (2 3 3), (1 3 0), (1 1 2), (3 0 1),
(0 2 2), (2 1 1), (3 3 2), (1 0 3) }
Number of codewords is 16.

Code L4: { (0 0 0), (2 0 0), (1 1 0), (3 1 0), (0 2 0), (2 2 0),
(1 3 0), (3 3 0), (1 0 1), (3 0 1), (0 1 1), (2 1 1),
(1 2 1), (3 2 1), (0 3 1), (2 3 1), (0 0 2), (2 0 2),
(1 1 2), (3 1 2), (0 2 2), (2 2 2), (1 3 2), (3 3 2),
(1 0 3), (3 0 3), (0 1 3), (2 1 3), (1 2 3), (3 2 3),
(0 3 3), (2 3 3) }
Number of codewords is 32.

this case message block length is one from each source. Similarly L4 is suitable as a code for two sources $S_{4,1}$ and $S_{4,2}$ with symbol size 2 and 4 respectively as shown in Fig 3.1(b). The message block lengths in this case are 1 for source $S_{4,1}$ and 2 for source $S_{4,2}$. This kind of situation does not arise in the case of linear codes over GF(p^m). That is, any linear code over finite fields can always be used for a single source. This is explained in Theorem 3.1.

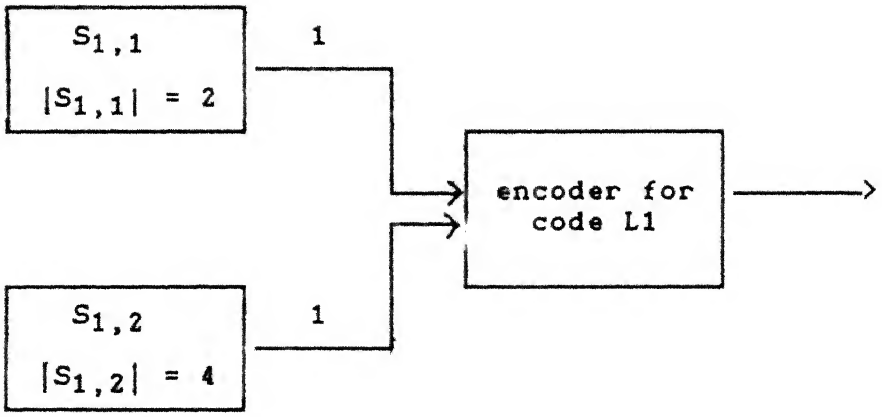


Fig 3.1(a) Code L1 for two sources $S_{1,1}$ and $S_{1,2}$.

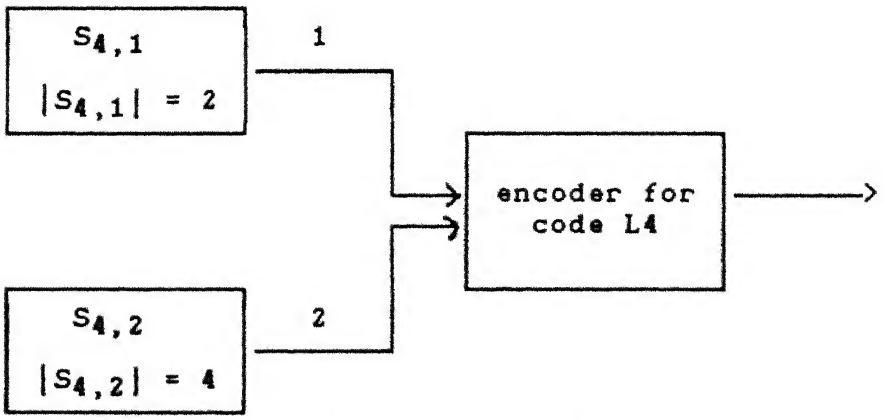


Fig 3.1(b) Code L4 for two sources $S_{4,1}$ and $S_{4,2}$.

Theorem 3.1: Let M denote the module of the set of n-tuples over Z_{p^k}. Then every submodule of M is isomorphic to a direct sum of n ideals of Z_{p^k}.

Proof: Let $(m_1,m_2,\ldots,m_n) \in M$ where $m_i \in Z_{p^k}$, $i=1,2,\ldots n$. The mapping $\emptyset_i(m_1,m_2,\ldots,m_n) = (0,0,..,m_i,..0)$ defines an isomorphism between M and n copies of Z_{p^k}. We have

$$M \equiv Z_{p^k} \oplus Z_{p^k} \oplus \ldots \oplus Z_{p^k} .$$

Let N be a submodule of M and $r = (r_1,r_2,\ldots,r_n) \in N$. Consider the set of i-th component r_i of all elements of N. Let it be $A_i = \{ r_{i_1}, r_{i_2}, \ldots\ldots \}$. Since N is a submodule over Z_{p^k} we have $Z_{p^k} A_i = A_i$ and hence A_i is an ideal of Z_{p^k}. From this it follows that $N \equiv A_1 \oplus A_2 \oplus \ldots \oplus A_n$. Q.E.D.

Let L be any linear code over Z_{p^k}. We have

$$L = I_1 \oplus I_2 \oplus \ldots \oplus I_n$$

where I_i is an ideal of Z_{p^k}. Ideals of Z_{p^k} are generated by p^j for $j=0,1,\ldots,k$. Let $I_i = p^{j_i} Z_{p^k}$. Then word-length of L is $j_1+j_2+\ldots+j_n$. Note that $0 \leq j_i \leq k$, $i=1,2,\ldots.n$, whereas in the case of codes over finite fields $GF(p^e)$ since the only ideals are trivial ideals each I_i is either $GF(p^e)$ or 0. i.e., j_i is equal to either 0 or e for all i. Hence word-length is a multiple of e, say ke, in which case k is called the dimension of the code.

The situation where certain linear codes over Z_{p^k} are suitable only for coding more than one source alphabet simultaneously is unique for the case of linear codes over Z_{p^k}, not seen in the case of linear codes over finite fields. In a strict sense, these codes can not be called codes over Z_{p^k} since at least one of the sources coded using these codes has alphabet size not equal to p^k. Since these codes arise as submodules of modules over Z_{p^k}, we call these codes linear codes over Z_{p^k} and do not distinguish these codes from the codes that can be used for a single source with alphabet Z_{p^k}.

3.2 CYCLIC CODES OVER Z_m

In this section various ways of studying cyclic codes are briefly discussed. Cyclic codes over Z_{p^k} are defined as follows:

Definition 3.3: A linear code C over Z_{p^k} is said to be a cyclic code if whenever $(a_0,a_1,\ldots,a_{n-1})$ is in C then $(a_{n-1},a_0,a_1,\ldots,a_{n-2})$ is also in C.

A cyclic code over Z_{p^k} can also be defined as an ideal of the residue class polynomial ring $Z_{p^k}[x]/(x^n-1)$ or equivalently as an ideal in an appropriate group ring. These equivalent definitions are briefly discussed in the following subsections.

3.2.1 Polynomial theoretic approach

For studying cyclic codes over Z_{p^k}, as in the case of cyclic codes over $GF(p^k)$, it is convenient to associate with every n-tuple over Z_{p^k}, $a = (a_0, a_1, \ldots, a_{n-1})$, the polynomial $a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \in Z_{p^k}[x]$. Assuming that $a(x) \in Z_{p^k}[x]$ modulo (x^n-1), multiplication of $a(x)$ by x corresponds to a cyclic shift. With this one-to-one correspondence between $Z_{p^k}^n$ and the ring $Z_{p^k}[x]/(x^n-1)$ a cyclic code over Z_{p^k} can be interpreted as an ideal in the ring $Z_{p^k}[x]/(x^n-1)$. Hence every zero divisor of the ring $Z_{p^k}[x]/(x^n-1)$ generates a cyclic code. In other words any polynomial of degree less than n that divides (x^n-1) generates a cyclic code. The difficulty in this approach is that (x^n-1) does not have a unique factorization in $Z_{p^k}[x]$, unlike in the case of polynomial ring over a finite field.

3.2.2 Group algebra approach

Let G_n denote the cyclic group of order n and $Z_{p^k}[G_n]$ the group ring of G_n over Z_{p^k}. We have

$$Z_{p^k}[G_n] = \{ \sum_{g \in G} a_g \, g : a_g \in Z_{p^k} \}$$

Let us associate with each codeword $a = (a_0, a_1, \ldots, a_{n-1})$ the element $\sum_{i=0}^{n-1} a_i \, g^i$, where g is a generator of the group G_n. Note that multiplication of an element of $Z_{p^k}[G_n]$ by g is equivalent

to cyclically shifting once the associated n-tuple over Z_{pk}. With this one-to-one correspondence between the set of n-tuples over Z_{pk} and $Z_{pk}[G_n]$, a cyclic code over Z_{pk} can be interpreted as an ideal in the group ring $Z_{pk}[G_n]$.

If the cyclic group G_n is replaced by an Abelian group then a class of codes called Abelian codes is obtained. This general class of codes over Z_{pk} is discussed in Chapter 5 in the transform domain.

3.2.3 Transform domain approach

Let us consider cyclic codes over GF(p^e). From the polynomial theoretic approach it is known that any polynomial of degree less than n that divides (x^n-1) generates a cyclic code over GF(p^e). Let g(x) denote the generator polynomial of a cyclic code. i.e., g(x) is a divisor of (x^n-1). If n and p are relatively prime, then it is possible to extend the field GF(p^e) to GF(p^{er}) such that the polynomial (x^n-1) factors into linear factors. Thus, in GF(p^{er}), we have

$$x^n-1 = (x-1)(x-\alpha)(x-\alpha^2)....(x-\alpha^{n-1})$$

Since g(x) is a factor of (x^n-1), the roots of g(x) belong to a subset of roots of x^n-1. The cyclic code is uniquely specified by the roots of the generator polynomial. Note that if β is a root

of $g(x)$ then β^p, β^{p^2}, β^{p^3},... are also the roots of $g(x)$.

When n and m are relatively prime cyclic codes over finite fields can be studied using DFT over extension fields as follows.

Definiton 3.4: Let $(a_0,a_1,\ldots,a_{n-1})$ be an n-tuple over $GF(p^e)$ and r be the least integer such that n divides $p^{er}-1$. Let α be an element of order n in $GF(p^{er})$. Then the DFT is defined by

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i \qquad j=0,1,\ldots,n-1.$$

The transform vector is $(A_0,A_1,\ldots,A_{n-1})$, where $A_0,A_1,\ldots A_{n-1}$ are elements of $GF(p^{er})$, and they are called the DFT coefficients of the vector $(a_0,a_1,\ldots,a_{n-1})$. The transform vector and the corresponding DFT coefficients are also respectively referred as spectrum and spectral coefficients or components.

It may be noted that A_j is equal to the value of $A(x)$ evaluated at $x=\alpha^j$. Hence if the generator polynomial $g(x)$ has roots $\alpha^{j_1},\alpha^{j_2},\ldots,\alpha^{j_r}$ then the corresponding DFT coefficients of $g(x)$, $G_{j_1},G_{j_2},\ldots,G_{j_r}$, will be identically equal to zero. Since every codeword is a multiple of $g(x)$, because of the convolution property of DFT, every codeword will have zero at the j-th component of its transform vector for all $j \in (j_1, j_2,\ldots, j_r)$. This leads to the definition of cyclic codes in the transform domain as follows.

Definition 3.5: A cyclic code over GF(q) is the set of n-tuples over GF(q) whose transform vectors have a specified set of components equal to zero.

Example 3.1: Consider the binary Hamming (7,4) code which is also cyclic with generator polynomial x^3+x^2+1. The extension field is GF(8) and let α denote a primitive element of GF(8). All the codewords with spectrum are listed in Table 3.2.

This transform domain approach for codes over finite fields is extended to cyclic and Abelian codes over Z_m in subsequent chapters.

Table 3.2 Listing of codewords and their spectrum corresponding to Example 3.1

Codewords							Spectrum						
a_0	a_1	a_2	a_3	a_4	a_5	a_6	A_0	A_1	A_2	A_3	A_4	A_5	A_6
0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	1	1	0	1	0	0	0	0	0	α^0	0	α^0	α^0
0	0	1	1	1	0	1	0	0	0	α^1	0	α^4	α^2
0	1	0	0	1	1	1	0	0	0	α^2	0	α^1	α^4
1	1	0	1	0	0	1	0	0	0	α^3	0	α^5	α^6
0	1	1	1	0	1	0	0	0	0	α^4	0	α^2	α^1
1	0	0	1	1	1	0	0	0	0	α^5	0	α^6	α^3
1	0	1	0	0	1	1	0	0	0	α^6	0	α^3	α^5
1	1	1	1	1	1	1	1	0	0	0	0	0	0
0	0	0	1	0	1	1	1	0	0	α^0	0	α^0	α^0
1	1	0	0	0	1	0	1	0	0	α^1	0	α^4	α^2
1	0	1	1	0	0	0	1	0	0	α^2	0	α^1	α^4
0	0	1	0	1	1	0	1	0	0	α^3	0	α^5	α^6
1	0	0	0	1	0	1	1	0	0	α^4	0	α^2	α^1
0	1	1	0	0	0	1	1	0	0	α^5	0	α^6	α^3
0	1	0	1	1	0	0	1	0	0	α^6	0	α^3	α^5

CHAPTER 4

CYCLIC CODES OVER Z_m

For any integer m, cyclic codes of length n over Z_m are ideals in the ring of polynomials with coefficients from Z_m modulo the polynomial (x^n-1). If $m = \prod_{i=1}^{s} p_i^{k_i}$, then we have the following isomorphisms.

$$Z_m \equiv \bigoplus_{i=1}^{s} Z_{p_i^{k_i}} \quad \text{and} \quad Z_m[x]/(x^n-1) \equiv \bigoplus_{i=1}^{s} Z_{p_i^{k_i}}[x]/(x^n-1) \qquad (4.1)$$

In Section 4.1, spectral characterisation for the case $m = p^k$ is obtained. The DFT defines an isomorphism between the ring $Z_{p^k}[x]/(x^n-1)$ with cyclic convolution as multiplication and a subring of the ring of n-tuples over $GR(p^k,r)$ with pointwise addition and multiplication. We identify this subring which is the image of all n-tuples over Z_{p^k} under DFT, using which spectral characterisation of cyclic codes over Z_{p^k} is obtained. Using isomorphisms given in (4.1), the results are extended to arbitrary m in Section 4.2. The special case of m being a product of distinct primes is considered in Section 4.3. In Section 4.4 BCH codes over Z_m are discussed.

4.1 SPECTRAL CHARACTERISATION FOR $m = p^k$

In this section cyclic codes over Z_{p^k} are discussed. In Subsection 4.1.1, DFT suitable for cyclic codes over Z_{p^k} is defined and in Subsection 4.1.2, the notion of degree of an element of a Galois ring is introduced. This notion is useful to decide whether a given element of a Galois ring is present in which subrings of the Galois ring. Spectral characterisation for cyclic codes over Z_{p^k} is obtained in Subsection 4.1.3. The notion of minimal and subminimal cyclic codes over Z_{p^k} is explained. The distance properties of cyclic codes over Z_{p^k}, both Hamming and Lee distance, are discussed in Subsection 4.1.4. In Subsection 4.1.5 a formula for word-length is obtained.

4.1.1 DFT for cyclic codes over Z_{p^k}

Cyclic codes over Z_{p^k} of length n are ideals in the residue class polynomial ring $Z_{p^k}[x]/(x^n-1)$. Given p^k and length n the DFT is constructed as follows. Choose the least integer r such that n divides (p^r-1). The required extension ring is $GR(p^k,r)$. From Fact 2.4 it follows that the group of units $GR^*(p^k,r)$ contains a cyclic subgroup G_1 whose order is (p^r-1). Further, since n divides (p^r-1) an element α exists in G_1 whose order is n. Hence $GR(p^k,r)$ supports a DFT of length n over Z_{p^k}.

Definition 4.1: Let $a = (a_0,a_1,\ldots,a_{n-1})$ be an n-tuple over Z_{p^k}. The DFT of a is defined as

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i \quad ; \quad j=0,1,\ldots,n-1$$

where α is an element of multiplicative order n in $GR(p^k,r)$, where r is the least integer such that n divides (p^r-1). The vector $A = (A_0,A_1,\ldots,A_{n-1})$ is called the transform vector or spectrum of $a = (a_0,a_1,\ldots,a_{n-1})$. The components A_i, $i=1,2,\ldots,n$, are called DFT coefficients or spectral components of a.

The DFT maps an element of $Z_{p^k}^n$ to an element of $GR^n(p^k,r)$. There are p^{kn} elements in $Z_{p^k}^n$ and p^{knr} elements in $GR^n(p^k,r)$. An element of $GR^n(p^k,r)$ which qualifys to be the image of some element of $Z_{p^k}^n$ under DFT is determined by conjugacy symmetry property. Identifying the structure of the set of these images under DFT is the key idea that helps us to obtain transform domain characterisation of cyclic codes over Z_{p^k}. Towards this end, we introduce the notion of degree of an element of a Galois ring in the following subsection.

4.1.2 Degree of an element of a Galois ring

Consider the Galois ring $GR(p^k,s)$. If r divides s, then $GR(p^k,s)$ contains a subring which is isomorphic to $GR(p^k,r)$. For our purposes it is required to identify the elements of $GR(p^k,s)$ which constitute the subring $GR(p^k,r)$.

Let us first consider the case of Galois fields. i.e., k = 1 in $GR(p^k,s)$. Let $GF(p^s)$ be the extension field of degree s over GF(p). If r divides s then $GF(p^s)$ contains a subfield isomorphic to $GF(p^r)$. Let

$$GF(p^s) = \{ 0,1,\alpha,\alpha^2,\alpha^3,.....,\alpha^{p^{s-3}}, \alpha^{p^{s-2}} \}$$

where α is a primitive element of $GF(p^s)$. Since r divides s, p^r-1 divides p^s-1. Let $p^s-1 = d(p^r-1)$ and consider the subset $\{ 0, 1, \alpha^d, \alpha^{2d}, \alpha^{3d},..., \alpha^{(p^r-1)d} \}$ of $GF(p^s)$. It can be shown that this subset is isomorphic to $GF(p^r)$. For example in $GF(2^6) = \{ 0, 1, \alpha, \alpha^2, ..., \alpha^{62} \}$, the subfield isomorphic to GF(2) is $\{ 0, 1 \}$, the subfield isomorphic to $GF(2^2)$ is $\{ 0, 1, \alpha^{21}, \alpha^{42} \}$ and the subfield isomorphic to $GF(2^3)$ is $\{ 0, 1, \alpha^9, \alpha^{18}, \alpha^{27}, \alpha^{36}, \alpha^{45}, \alpha^{54} \}$. This method fails in Galois rings because every nonzero element in it is not necessarily a unit.

To identify a subring in a Galois ring, we shall use the fact that there is a one-to-one correspondence between the subgroups of the automorphism group of a Galois ring and the set of subrings of the Galois ring [24]. The subgroup of the automorphism group that corresponds to a particular subring of the Galois ring consists of those automorphisms which leave the elements of the subring invariant. Let the generator of the automorphism group be σ: $\sigma(\alpha) = \alpha^p$. It is clear that if $\beta \in GR(p^k,r)$ but not in any subring $GR(p^k,r_1)$, where $r_1 < r$ then the least integer t such that $\sigma^t(\beta) = \beta$ is equal to r.

Definition 4.2: Let β be an element of the Galois ring $GR(p^k,s)$. The degree of β is defined as the least integer r such that $\sigma^r(\beta) = \beta$, where σ is a generator of the group of automorphisms of $GR(p^k,s)$.

Since the set $\{0,1,2,\ldots,p^k-1\}$ is invariant under the group of automorphisms of $GR(p^k,s)$, it follows that this set, isomorphic to Z_{p^k} in $GR(p^k,s)$, consists of elements of degree 1. Moreover the subring of $GR(p^k,s)$ which is isomorphic to $GR(p^k,r)$, where r divides s, consists of the elements of $GR(p^k,s)$ whose degree divides r.

Example 4.1: Consider $GR(4,4) \equiv Z_4[x]/(x^4+x+1)$. Every element is of the form $a_0+a_1x+a_2x^2+a_3x^3$. The mapping σ : $\sigma(x) = 2+2x+3x^2$ is a generator of the automorphism group of $GR(4,4)$. Degree of an element can be 1,2 or 4.

(a) The elements of degree 1 are 0,1,2 and 3.

(b) The elements of degree 2 are

$1+2x+2x^2$, $2x+2x^2$, $2+2x+2x^2$, $3+2x+2x^2$, $3x+x^2+2x^3$, $1+3x+x^2+2x^3$, $2+3x+x^2+2x^3$, $3+3x+x^2+2x^3$, $x+3x^2+2x^3$, $1+x+3x^2+2x^3$, $2+x+3x^2+2x^3$, and $3+x+3x^2+2x^3$.

(c) All other elements are of degree 4.

4.1.3 Spectral characterisation

The basis for the spectral characterisation of cyclic codes over Z_{p^k} is the following theorem.

Theorem 4.1: Let R_T denote the subset of $GR^n(p^k,r)$ which is the set of transform vectors of all n-tuples over Z_{p^k}. Then

$$R_T \equiv \bigoplus_{i=1}^{t} GR(p^k,r_i)$$

where t is the number of conjugacy classes for the integer n and the prime p and r_i, i=1,2,...,t, are the exponents of the conjugacy classes.

Proof: For a fixed j, $0 \leq j < n$, let the conjugacy class $C_{p,n}(j)$ have exponent e. For any element $(A_0,A_1,..,A_{n-1})$ of R_T, because of the conjugate symmetry property it is required that

$$\sigma(A_{p^{e-1}j}) = A_{p^e j} ,$$

i.e., $\sigma^e(A_k) = A_k$ for all k in the conjugacy class $C_{p,n}(j)$. In other words A_k is an element of degree e and hence belongs to the subring $GR(p^k,e)$. Let R_{T_j} denote the subset of R_T consisting of only those elements of R_T which have all spectral components zero except the ones that belong to $C_{p,n}(j)$. Since the value of one spectral component of a conjugacy class uniquely specifies the values at other components in the conjugacy class given by the conjugacy symmetry property, it follows that

$$R_{T_j} \equiv GR(p^k, e).$$

Moreover, since the conjugacy classes are disjoint and operations in R_T are pointwise it follows that

$$R_T \equiv R_{T_{j_1}} \oplus R_{T_{j_2}} \oplus \ldots \oplus R_{T_{j_t}}$$

where $j_1, j_2, \ldots, j_t$ belong to different conjugacy classes and t is the number of conjugacy classes. From the above isomorphisms it follows that

$$R_T \equiv \bigoplus_{i=1}^{t} GR(p^k, r_i)$$

where t is the number of conjugacy classes and r_i is the exponent of the i-th conjugacy class. Q.E.D.

From the above theorem and the convolution property of the DFT it follows that

$$Z_{p^k}[x]/(x^n-1) \equiv \bigoplus_{i=1}^{t} GR(p^k, r_i)$$

This means there is a one-to-one correspondence between the ideals of $Z_{p^k}[x]/(x^n-1)$ which are in fact cyclic codes of length n over Z_{p^k} and ideals of $\bigoplus_{i=1}^{t} GR(p^k, r_i)$. For all i, i=1,2,..,t, all the ideals of $GR(p^k, r_i)$ are known. In fact the ideals are $p^j GR(p^k, r_i)$, j = 0,1,...,k. Hence cyclic codes over Z_{p^k} can be characterised in terms of spectral components as follows:

Definition 4.3: For an integer n and a prime p let there be t conjugacy classes with exponents r_i, i=1,2,...,t. Let r be the least integer such that n divides p^r-1. A cyclic code of length n

over Z_{p^k} consists of the inverse DFT coefficients of all vectors of the subring $\bigoplus_{i=1}^{t} GR(p^k,r_i)$ of $GR^n(p^k,r)$ whose specified spectral components take values from an ideal $p^jGR(p^k,r_i)$, $0 \leq j \leq k$, for i=1,2,...,t. In other words any cyclic code L over Z_{p^k} is of the form

$$L \equiv \bigoplus_{i=1}^{t} p^{j_i}GR(p^k,r_i) \quad ; \qquad 0 \leq j_i \leq k$$

Example 4.2: Let n=3 and $m=2^2$. We have r=2 and the extension ring in which DFT is defined is GR(4,2). Every element of GR(4,2) is of the form a+bx where $a,b \in Z_4$. Let us denote a+bx by the ordered 2-tuple ab.

$$Z_4[x]/(x^3-1) \equiv GR(4,1) \oplus GR(4,2)$$
$$\equiv Z_4 \oplus GR(4,2)$$

Ideals of GR(4,2) are {(00)}, {00,02,20,22}and GR(4,2). Ideals of GR(4,1) are {00}, {00,20} and {00,10,20,30}. The transform matrix has already been given in Example 2.5. The conjugacy classes are {0} and {1,2}. The conjugacy class {0} can take values from ideals of GR(4,1) and the conjugacy class {1,2} can take values from the ideals of GR(4,2). The codwewords of all cyclic codes and their spectrum are listed in Table 4.1 in the next page.

Example 4.3: Let n=3 and $m=2^3$. Appropriate extension ring is GR(8,2). The irreducible polynomial of degree 2 over $Z_8[x]$ chosen to construct GR(8,2) is (x^2+x+1). The transform factor is x, and the transform matrix is

Table 4.1 Listing of codewords and spectrum of all cyclic codes of length 3 over Z_4.

codewords a_0 a_1 a_2	spectrum A_0 A_1 A_2	codewords a_0 a_1 a_2	spectrum A_0 A_1 A_2	codewords a_0 a_1 a_2	spectrum A_0 A_1 A_2
Code N1:					
0 0 0	00 00 00	2 2 2	20 00 00		
Code N2:					
0 0 0	00 00 00	2 2 0	00 22 02	0 2 2	00 20 20
2 0 2	00 02 22				
Code N3:					
0 0 0	00 00 00	1 1 1	30 00 00	2 2 2	20 00 00
3 3 3	10 00 00				
Code N4:					
0 0 0	00 00 00	2 0 0	20 20 20	0 2 0	20 02 22
2 2 0	00 22 02	0 0 2	20 22 02	2 0 2	00 02 22
0 2 2	00 20 20	2 2 2	20 00 00		
Code N5:					
0 0 0	00 00 00	3 1 0	00 31 23	2 2 0	00 22 02
1 3 0	00 13 21	3 0 1	00 23 31	2 1 1	00 10 10
1 2 1	00 01 33	0 3 1	00 32 12	2 0 2	00 02 22
1 1 2	00 33 01	0 2 2	00 20 20	3 3 2	00 11 03
3 2 3	00 03 11	2 3 3	00 30 30	1 0 3	00 21 13
0 1 3	00 12 32				
Code N6:					
0 0 0	00 00 00	0 2 0	20 02 22	1 1 1	30 00 00
2 0 0	20 20 20	3 1 1	10 20 20	2 0 2	00 02 22
1 3 1	10 02 22	3 3 1	30 22 02	0 0 2	20 22 02
0 2 2	00 20 20	2 2 2	20 00 00	1 1 3	10 22 02
3 1 3	30 02 22	1 3 3	30 20 20	3 3 3	10 00 00
2 2 0	00 22 02				
Code N7:					
0 0 0	00 00 00	2 0 0	20 20 20	1 1 0	20 11 03
3 1 0	00 31 23	0 2 0	20 02 22	2 2 0	00 22 02
1 3 0	00 13 21	3 3 0	20 33 01	1 0 1	20 03 11
3 0 1	00 23 31	0 1 1	20 30 30	2 1 1	00 10 10
1 2 1	00 01 33	3 2 1	20 21 13	0 3 1	00 32 12
2 3 1	20 12 32	2 3 3	00 30 30	0 3 3	20 10 10
0 0 2	20 22 02	2 0 2	00 02 22	1 1 2	00 33 01
3 1 2	20 13 21	0 2 2	00 20 20	2 2 2	20 00 00
1 3 2	20 31 23	3 3 2	00 11 03	1 0 3	00 21 13
3 0 3	20 01 33	0 1 3	00 12 32	2 1 3	20 32 12
1 2 3	20 23 31	3 2 3	00 03 11		

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & x & 7+7x \\ 1 & 7+7x & x \end{bmatrix}$$

We have

$$Z_8[x]/(x^3-1) \equiv GR(8,1) \oplus GR(8,2)$$

$$\equiv Z_8 \oplus GR(8,2)$$

Ideals of GR(8,1) are (00), (00,40), (00,20,40,60) and (00,10,20,30,40,50,60,70). Ideals of GR(8,2) are (00), 2GR(8,2), 4GR(8,2) and GR(8,2). The conjugacy classes are (0) and (1,2). The codewords of all the cyclic codes and their spectrum are listed in Appendix A.

4.1.4 Minimal and subminimal cyclic codes

In what follows we identify a set of cyclic codes over Z_{p^k} from which all other cyclic codes over Z_{p^k} can be obtained.

In the case of cyclic codes over finite fields there are codes called minimal cyclic codes, the direct sums of which give all cyclic codes. Similar codes in the case of cyclic codes over Z_{p^k}, called minimal codes and subminimal codes, are defined from which all other codes can be obtained as direct sums of these codes.

From definition 4.3 any cyclic code L, over Z_{p^k}, is of the form

$$L \equiv \bigoplus_{i=1}^{t} p^{j_i} GR(p^k, r_i) \quad ; \qquad 0 \leq j_i \leq k$$

Definition 4.4: Given Z_{p^k} and code length n, the cyclic codes L_i, i=1,2,...,t, given by

$$L_i \equiv GR(p^k, r_i)$$

are called minimal codes and cyclic codes

$$L_{i,j} \equiv p^{j_i} GR(p^k, r_i) \quad ; \qquad 0 < j_i < k,$$

are called subminimal codes corresponding to L_i. The minimal code L_i is denoted also by $L_{i,0}$.

Every minimal cyclic code is isomorphic to a Galois ring. When k = 1, this reduces to the well known fact, that every minimal cyclic code over GF(q) is isomorphic to a finite field. Minimal codes are cyclic codes with one conjugacy class (say i-th conjugacy class) taking values from $GR(p^k, r_i)$ and zeros in all other conjugacy classes. Subminimal cyclic codes are cyclic codes with one conjugacy class taking values from an ideal $p^{j_i} GR(p^k, r_i)$, $0 < j_i < k$, of the Galois ring corresponding to the conjugacy class, and zeros in all other conjugacy classes. It follows from the local ring structure of Galois ring that every subminimal cyclic code is a subcode of the corresponding minimal code. Explicitly, there is the following chain structure of subminimal codes corresponding to L_i,

$$p^{k-1}GR(p^k,r_i) \subset p^{k-2}GR(p^k,r_i) \subset \ldots\ldots \subset p^2GR(p^k,r_i) \subset pGR(p^k,r_i)$$

i.e, $$L_{i,k-1} \subset L_{i,k-2} \subset \ldots\ldots\ldots \subset L_{i,2} \subset L_{i,1}$$

Since any cyclic code L over Z_{p^k} is of the form

$$L \equiv \bigoplus_{i=1}^{t} p^{j_i}GR(p^k,r_i)$$

we have

$$L \equiv \bigoplus_{i=1}^{t} L_{i,j_i}$$

Hence every cyclic code over Z_{p^k} is a direct sum of some minimal and subminimal codes.

In finite field case, because of the absence of nontrivial ideals, counterpart of subminimal cyclic codes over Z_{p^k} do not exist.

Now calculating the number of nontrivial cyclic codes is straight forward. From Definition 4.4 it follows that there are $(k+1)^t-2$ nontrivial cyclic codes of length n over Z_{p^k} since each direct summand $GR(p^k,r_i)$ has (k+1) ideals $p^jGR(p^k,r_i)$, j=0,1,...,k.

Example 4.4: The minimal and subminimal codes corresponding to Examples 4.2 and 4.3, and their direct sum giving other cyclic codes are illustrated.

(i) The minimal codes for length 3 cyclic codes over Z_4 are codes N3 and N5 (Refer Table 4.1). The subminimal codes corresponding to N3 is N1 and corresponding to N5 is N2. The code N4 is the direct sum of N1 and N2 , the code N6 is the direct sum of N2 and N3 and the code N7 is the direct sum of N1 and N5.

(ii) The minimal codes for length 3 cyclic codes over Z_8 are codes N5 and N11 (Refer Appendix A). The subminimal codes corresponding to N5 are N1 and N3. The subminimal codes corresponding to N11 are N2 and N6. Other codes in terms of the direct sum of these codes are as follows.

N4 ≡ N1 ⊕ N2

N7 ≡ N2 ⊕ N3

N8 ≡ N1 ⊕ N6

N9 ≡ N5 ⊕ N2

N10 ≡ N3 ⊕ N6

N12 ≡ N1 ⊕ N11

N13 ≡ N5 ⊕ N6

N14 ≡ N3 ⊕ N11

4.1.5 Metric for codes over Z_{p^k}

The choice of metric depends on the criterion of decoding and channel [29]. Both Hamming and Lee metric can be used for codes over Z_m. If the minimum distance of a code is 2t+1, then it can correct upto t errors.

In this subsection we point out that, for the same number of codewords, in certain cases, codes over Z_{p^k} with DFT coefficients from nontrivial ideals of extension ring have greater Lee distance compared to codes with DFT coefficients from only trivial ideals. No general result regarding this has been obtained. Our purpose here is to point out that codes with DFT coefficients from nontrivial ideals of the extension ring have some desirable properties. As far as Hamming distance is concerned it is observed that nontrivial ideals in conjugacy classes instead of full ring in those conjugacy classes do not change the minimum Hamming distance of the code.

We list below the codewords and DFT coefficients of two codes from Example 4.2 of the previous section, both having four codewords of length 3 over Z_4.

code 1

codeword	spectrum
$(a_0\ a_1\ a_2)$	$(A_0\ A_1\ A_2)$
0 0 0	00 00 00
2 0 2	00 02 22
2 2 0	00 20 02
0 2 2	00 20 20

code 2

codeword	spectrum
$(a_0\ a_1\ a_2)$	$(A_0\ A_1\ A_2)$
0 0 0	00 00 00
1 1 1	30 00 00
2 2 2	20 00 00
3 3 3	10 00 00

Code 1 has Lee distance 4, whereas code 2 has Lee distance 3.

In codes of length 3 over Z_8 also similar case can be seen. The two codes with eight codewords, one with nontrivial ideal in

both the conjugacy classes and the other one with trivial ideals in both conjugacy classes, are listed below (see Example 4.3).

code 1

codeword			spectrum		
$(a_0$	a_1	$a_2)$	$(A_0$	A_1	$A_2)$
0	0	0	00	00	00
4	0	0	40	40	40
4	0	4	00	04	44
0	4	0	40	04	44
0	4	4	00	40	40
4	4	0	00	44	04
0	0	4	40	44	04
4	4	4	40	00	00

code 2

codeword			spectrum		
$(a_0$	a_1	$a_2)$	$(A_0$	A_1	$A_2)$
0	0	0	00	00	00
1	1	1	30	00	00
2	2	2	60	00	00
3	3	3	10	00	00
4	4	4	40	00	00
5	5	5	70	00	00
6	6	6	20	00	00
7	7	7	40	00	00

It is seen that code 1 has Lee distance four whereas code 2 has Lee distance three.

In both the cases given above the repetition codes can be found. To show that this increase in Lee distance can occur in other cases also, we give below listing of three codes of length 4 over Z_9, all of them with 81 codewords. The conjugacy classes are $C_{3,4}(0) = \{ 0 \}$, $C_{3,4}(1) = \{ 1,3 \}$ and $C_{3,4}(2) = \{ 2 \}$. The extension ring is $GR(9,2) \equiv Z_9[x]/(x^2+x+1)$. The transform matrix is

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 2+4x & 8 & 7+5x \\ 1 & 8 & 1 & 8 \\ 1 & 7+5x & 8 & 2+4x \end{bmatrix}$$

We have

$$Z_9[x]/(x^4-1) \equiv GR(9,1) \oplus GR(9,1) \oplus GR(9,2).$$

The ideals of GR(9,2) are $3^0GR(9,2)$, $3GR(9,2)$ and $3^2GR(9,2) = 0$. Code 1 takes values from ideals 0,GR(9,2) and 0 respectively for the conjugacy classes $C_{3,4}(0)$, $C_{3,4}(1)$ and $C_{3,4}(2)$. Code 2 takes values from ideal 3GR(9,2) for all the conjugacy classes. Code 3 takes values from ideals 0, 3GR(9,2) and GR(9,2) respectively for conjugacy classes $C_{3,4}(0)$, $C_{3,4}(1)$ and $C_{3,4}(2)$. It is easy to check that the minimum Lee distance of code 1 is 2, and minimum Lee distance for code 2 is 3 and for code 3 it is 4. A complete listing of all codewords and their spectrum is given in Tables 4.2, 4.3 and 4.4.

As far as Hamming distance is concerned cyclic codes with elements from nonzero ideals in some conjugacy classes have the same minimum distance as codes with full ring in those conjugacy classes, all other conjugacy classes having zeros in both the codes. This is proved in the following theorems.

Theorem 4.2: Let two cyclic codes M_1 and M_2 over Z_{p^k} of same length with minimum Hamming distances d_1 and d_2 respectively be

$$M_1 \equiv p^{j_1}GR(p^k,r_i) \text{ and } M_2 \equiv p^{j_2}GR(p^k,r_i)$$

for some i, where $0 \leq j_1 < k$ and $0 \leq j_2 < k$. i.e., M_1 and M_2 are minimal codes or subminimal codes corresponding to a minimal code. Then d_1 and d_2 are equal.

Table 4.2 Codewords and spectrum of length 4 cyclic code over Z_9 defined by zero ideal in $C_{3,4}(0)$ and $C_{3,4}(2)$ and the ideal GR(9,2) in $C_{3,4}(1)$.

code 1

$(a_0$	a_1	a_2	$a_3)$	$(A_0$	A_1	A_2	$A_3)$	$(a_0$	a_1	a_2	$a_3)$	$(A_0$	A_1	A_2	$A_3)$
0	0	0	0	00	00	00	00	1	7	8	2	00	32	00	17
8	0	1	0	00	70	00	70	5	6	4	3	00	73	00	46
3	0	6	0	00	60	00	60	0	5	0	4	00	24	00	75
7	8	2	1	00	11	00	08	4	5	5	4	00	14	00	65
2	8	7	1	00	01	00	88	8	4	1	5	00	55	00	04
6	7	3	2	00	42	00	27	3	4	6	5	00	45	00	84
7	3	2	6	00	86	00	23	2	3	7	6	00	76	00	13
6	2	3	7	00	27	00	42	1	2	8	7	00	17	00	32
5	1	4	8	00	58	00	61	7	0	2	0	00	50	00	50
2	0	7	0	00	40	00	40	6	8	3	1	00	81	00	78
1	8	8	1	00	71	00	68	5	7	4	2	00	22	00	07
0	6	0	3	00	63	00	36	4	6	5	3	00	53	00	26
8	5	1	4	00	04	00	55	3	5	6	4	00	84	00	45
7	4	2	5	00	35	00	74	2	4	7	5	00	25	00	64
6	3	3	6	00	66	00	03	1	3	8	6	00	56	00	83
5	2	4	7	00	07	00	22	0	1	0	8	00	48	00	51
4	1	5	8	00	38	00	41	6	0	3	0	00	30	00	30
1	0	8	0	00	20	00	20	5	8	4	1	00	61	00	58
0	7	0	2	00	12	00	87	4	7	5	2	00	02	00	77
8	6	1	3	00	43	00	16	3	6	6	3	00	33	00	06
7	5	2	4	00	74	00	36	2	5	7	4	00	54	00	25
6	4	3	5	00	15	00	54	1	4	8	5	00	05	00	44
5	3	4	6	00	46	00	73	0	2	0	7	00	87	00	12
4	2	5	7	00	77	00	02	8	1	1	8	00	28	00	31
3	1	6	8	00	18	00	21	5	0	4	0	00	10	00	10
0	8	0	1	00	51	00	48	4	8	5	1	00	41	00	38
8	7	1	2	00	82	00	67	3	7	6	2	00	72	00	57
7	6	2	3	00	23	00	86	2	6	7	3	00	13	00	76
6	5	3	4	00	54	00	15	1	5	8	4	00	44	00	05
5	4	4	5	00	85	00	34	0	3	0	6	00	36	00	63
4	3	5	6	00	26	00	53	8	2	1	7	00	67	00	82
3	2	6	7	00	57	00	72	7	1	2	8	00	08	00	11
2	1	7	8	00	88	00	01	4	0	5	0	00	80	00	80
8	8	1	1	00	31	00	28	3	8	6	1	00	21	00	18
7	7	2	2	00	62	00	47	2	7	7	2	00	52	00	37
6	6	3	3	00	03	00	66	1	6	8	3	00	83	00	56
5	5	4	4	00	34	00	85	0	4	0	5	00	75	00	24
4	4	5	5	00	65	00	14	8	3	1	6	00	16	00	43
3	3	6	6	00	06	00	33	7	2	2	7	00	47	00	62
2	2	7	7	00	37	00	52	6	1	3	8	00	78	00	81
1	1	8	8	00	68	00	71								

Table 4.3 Codewords and spectrum of length 4 cyclic code over Z_9 defined by the ideal 3GR(9,2) in $C_{3,4}(1)$ and zero ideal in other conjugacy classes.

code 2

$(a_0$	a_1	a_2	$a_3)$	$(A_0$	A_1	A_2	$A_3)$	$(a_0$	a_1	a_2	$a_3)$	$(A_0$	A_1	A_2	$A_3)$
0	0	0	0	00	00	00	00	3	0	0	0	30	30	30	30
0	6	0	0	60	36	30	60	3	6	0	0	00	66	60	03
6	0	3	0	00	30	00	30	0	3	3	0	60	33	00	06
3	6	3	0	30	36	00	63	6	6	3	0	60	66	30	03
0	3	6	0	00	03	30	66	3	3	6	0	30	33	60	06
6	6	6	0	00	36	60	63	0	0	0	3	30	36	60	63
3	3	0	3	00	30	60	30	6	3	0	3	30	60	00	60
0	0	3	3	60	06	00	33	3	0	3	3	00	36	30	63
6	3	3	3	60	30	30	30	0	6	3	3	30	33	30	06
3	0	6	3	30	06	60	33	6	0	6	3	60	36	00	63
0	3	0	0	30	63	60	36	3	3	0	0	60	03	00	66
6	6	0	0	30	06	00	33	0	0	3	0	30	60	30	60
3	3	3	0	00	63	30	36	6	3	3	0	30	03	60	66
0	0	6	0	60	30	60	30	3	0	6	0	00	60	00	60
6	3	6	0	60	63	00	36	0	6	6	0	30	66	00	03
3	0	0	3	60	66	00	03	6	0	0	3	00	06	30	33
0	6	0	3	00	63	00	36	3	6	0	3	30	03	30	66
6	0	3	3	30	66	60	03	0	3	3	3	00	60	60	60
3	6	3	3	60	63	60	36	6	6	3	3	00	03	00	60
0	3	6	3	30	30	00	30	3	3	6	3	60	60	30	60
6	3	0	0	00	33	30	06	3	0	3	0	60	00	60	00
0	6	3	0	00	06	60	33	6	0	6	0	30	00	30	00
3	6	6	0	60	06	30	33	0	3	0	3	60	00	30	00
6	6	0	3	60	33	60	06	3	3	3	3	30	00	00	00
0	0	6	3	00	66	30	03	6	3	6	3	00	00	60	00
0	6	6	3	60	03	60	66	6	0	0	6	30	33	00	06
3	6	0	6	60	30	00	30	0	3	3	6	30	06	30	33
6	6	3	6	30	30	60	30	3	3	6	6	00	06	00	33
3	6	6	3	00	33	00	06	0	3	0	6	00	36	00	63
6	6	0	6	00	60	30	60	3	3	3	6	60	36	60	63
0	0	6	6	30	03	00	66	6	3	6	6	30	36	30	63
6	6	6	3	30	63	30	36	3	3	0	6	30	66	30	03
0	0	3	6	00	33	60	06	6	3	3	6	00	66	00	03
3	0	6	6	60	33	30	06	0	6	6	6	00	30	30	30
0	0	0	6	60	63	30	36	6	3	0	6	60	06	60	33
3	0	3	6	30	63	00	36	0	6	3	6	60	60	00	60
6	0	6	6	00	63	60	36	3	6	6	6	30	60	60	60
3	0	0	6	00	03	60	66	0	6	0	6	30	00	60	00
6	0	3	6	60	03	30	66	3	6	3	6	00	00	30	00
0	3	6	6	60	66	60	03	6	6	6	6	60	00	00	00
6	0	0	0	60	60	60	60								

Table 4.4 Codewords and spectrum of length 4 cyclic code over Z_9 defined by the zero ideal, the ideal 3GR(9,2) and the ideal GR(9,1) in $C_{3,4}(0)$, $C_{3,4}(1)$ and $C_{3,4}(2)$ respectively.

code 3

$(a_0$	a_1	a_2	$a_3)$	$(A_0$	A_1	A_2	$A_3)$	$(a_0$	a_1	a_2	$a_3)$	$(A_0$	A_1	A_2	$A_3)$
0	0	0	0	00	00	00	00	6	3	0	0	00	33	30	06
3	0	6	0	00	60	00	60	8	7	2	1	00	06	20	33
5	4	8	1	00	33	80	06	1	2	4	2	00	60	10	60
1	8	7	2	00	66	70	03	0	3	3	3	00	60	60	60
2	1	2	4	00	36	80	63	2	7	5	4	00	33	50	06
7	5	1	5	00	60	70	60	4	2	7	5	00	06	40	33
6	6	0	6	00	60	00	33	5	1	5	7	00	63	20	36
5	7	8	7	00	60	80	60	1	5	4	8	00	06	10	33
3	6	0	0	00	66	60	03	0	3	6	0	00	03	30	66
2	1	5	1	00	60	50	60	2	7	8	1	00	66	20	03
7	5	4	2	00	03	40	66	6	0	0	3	00	06	30	33
6	6	3	3	00	03	00	66	8	4	2	4	00	60	20	60
5	1	8	4	00	06	80	33	4	8	1	5	00	03	10	66
1	5	7	5	00	30	70	30	0	0	3	6	00	33	60	06
0	6	6	6	00	30	30	30	2	4	5	7	00	06	50	33
7	2	1	8	00	33	70	06	7	8	4	8	00	30	40	30
6	0	3	0	00	30	00	30	6	6	6	0	00	36	60	63
8	4	5	1	00	03	80	66	4	2	1	2	00	30	10	30
4	8	4	2	00	36	70	63	3	3	0	3	00	30	60	30
0	0	6	3	00	66	30	03	5	7	2	4	00	03	50	66
2	4	8	4	00	30	20	30	7	2	4	5	00	66	40	03
7	8	7	5	00	63	10	36	6	3	3	6	00	66	00	03
8	1	2	7	00	33	20	06	8	7	5	7	00	30	80	30
4	5	1	8	00	66	10	03	1	2	7	8	00	03	70	66
3	3	3	0	00	63	30	36	5	1	2	1	00	30	50	30
5	7	5	1	00	36	20	63	1	5	1	2	00	63	40	36
7	2	7	2	00	00	10	00	0	6	0	3	00	63	00	36
6	3	6	3	00	00	60	00	8	1	5	4	00	00	80	03
8	7	8	4	00	63	50	36	4	5	4	5	00	00	70	00
3	0	0	6	00	03	60	66	3	6	3	6	00	00	30	00
5	4	2	7	00	66	50	03	2	1	8	7	00	03	20	66
1	8	1	8	00	00	40	00	7	5	7	8	00	36	10	63
0	6	3	0	00	06	60	33	2	4	2	1	00	63	80	36
8	1	8	1	00	00	50	00	7	8	1	2	00	06	70	33
4	5	7	2	00	33	40	06	3	0	3	3	00	36	30	63
3	6	6	3	00	33	00	06	5	4	5	4	00	00	20	00
1	2	1	5	00	36	40	63	1	8	4	5	00	33	10	06
0	3	0	6	00	36	00	63	6	0	6	6	00	63	60	36
2	7	2	7	00	00	80	00	8	4	8	7	00	36	50	63
4	2	4	8	00	63	70	36	4	8	7	8	00	60	40	60
3	3	6	6	00	06	00	33								

Proof: If $j_1 = j_2$, then M_1 and M_2 are same and hence $d_1 = d_2$. If $j_1 \neq j_2$, let $j_1 > j_2$. Then M_1 is a subcode of M_2 and it follows that $d_1 \geq d_2$. Our aim is to prove that $d_1 = d_2$. It is sufficient if we prove this for the case $j_1 = j_2+1$.

Suppose $d_1 > d_2$. We have

$$\begin{aligned} pM_2 &= pp^{j_2}GR(p^k, r_i) \\ &= p^{j_1}GR(p^k, r_i) \\ &= M_1 \end{aligned}$$

Since $d_1 > d_2$, there is a codeword $a = (a_0, a_1, \ldots, a_{n-1})$ in M_2, with Hamming distance d_2, which is not in M_1. Consider the vector $b = pa = (pa_0, pa_1, \ldots, pa_{n-1})$. If b is not a all zero vector, then since $pM_2 = M_1$ and $a \in M_2$, we have $b \in M_1$. Let the Hamming distance of $b = d_3$. We have $d_3 \leq d_2$. But $d_2 < d_1$. Hence $d3 < d1$. This contradicts the minimality of d_1. Hence $d_1 = d_2$. It remains to prove that $b = pa$ is not a all zero vector.

Let j be the minimum of powers of p in the expression of all components of a in the form up^t where u is a unit. (Note that for a zero component t=k.) Suppose b is a all zero vector. Then we have $j = k-1$. This means, since $a \in M2$, $j_2 \geq k-1$. Since $j_2 < k$, we have $j_2 = k-1$. Since $j_1 = j_2+1$, we have $j_1 = k$. This is not possible since $j_1 < k$. Hence b is not a all zero vector. Q.E.D.

Theorem 4.3: Let M_1 and M_2 be two cyclic codes over Z_{p^k} of same length with zeros in the same set of conjugacy classes and nonzeros in other conjugacy classes. Irrespective of the ideals

from which nonzero values are assumed, M_1 and M_2 have the same minimum distance.

Proof: Let M_1 and M_2 be cyclic codes over Z_{p^k}, given by

$$M_1 \equiv \bigoplus_{i=1}^{t'} p^{j_i} GR(p^k, r_i), \quad 0 \leq j_i < k, \ i=1,2,\ldots,t'$$

and

$$M_2 \equiv \bigoplus_{i=1}^{t'} p^{j'_i} GR(p^k, r_i), \quad 0 \leq j'_i < k, \ i=1,2,\ldots,t'.$$

Let d_1, and d_2 be respectively the minimum Hamming distances of M_1, and M_2. Our aim is to prove that $d_1 = d_2$.

Let M be the cyclic code given by

$$M \equiv \bigoplus_{\substack{i=1 \\ i \neq u}}^{t'} p^{j_i} GR(p^k, r_i) \oplus p^{j_u - 1} GR(p^k, r_u)$$

for some $u \in \{1,2,\ldots,t'\}$. Let the minimum Hamming distance of M be d. It is sufficient if we prove d = d1. Because, by proving d = d1, we prove that two cyclic codes with values from nonzero ideals in the same set of conjugacy classes and same nonzero ideals in all the conjugacy classes except in one in which the ideals are such that one can be obtained from the other one by multiplying by p.

Clearly M_1 is contained in M. Hence $d \leq d_1$. Suppose $d < d_1$. Let $a = (a_0, a_1, \ldots, a_{n-1})$ be a codeword in M of Hamming distance d, and a is not in M_1. Define $b = pa = (pa_0, pa_1, \ldots, pa_{n-1})$. Clearly pa is a codeword in M_1. Multiplication by p of a cannot increase the Hamming distance of a. Hence Hamming distance of $b \leq d$. We assume that b is not a all zero vector. Since b is in M_1, minimality of d_1 is contradicted. Hence $d = d_1$. It remains to

prove that b is not a all zero vector.

Let j be the minimum of powers of p in the expression of all components of a in the form up^t where u is a unit. Suppose b is a all zero vector. Then we have $j = k-1$. This means, in the transform vector of a, say $(A_0,A_1,\ldots,A_{n-1})$, the components corresponding to the u-th conjugacy class belong to $p^{k-1}GR(pk,r)$. Since $a \in M$, we have $j_u-1 = k-1$, which means $j_u = k$. But by definition of M_1, we have $j_u < k$. Hence b is not a all zero vector. Q.E.D.

A set of tables is given in Appendix C which lists all the cyclic codes with minimum Hamming and Lee distance and the number of codewords for the following cases:

(1) length 3 over Z_4

(2) length 5 over Z_4

(3) length 7 over Z_4

(4) length 4 over Z_9

(5) length 3 over Z_8

4.1.6 Formula for word-length

In the case of finite fields, say GF(q), if the dimension of a linear code C is k, then the number of codewords in C is q^k. It was seen in Section 3.1 that if L is a linear code over Z_{p^k} then the number of codewords in L is p^{μ}, where μ is the word-length of L. In this subsection we obtain a formula for word-length for cyclic codes over Z_{p^k} in terms of exponents of the conjugacy classes and the ideals from which the conjugacy classes take values.

Let us consider the cyclic codes of length n over Z_{p^k}. Let there be t conjugacy classes, $C_{p,n}(i_1)$, $C_{p,n}(i_2)$, ..., $C_{p,n}(i_t)$, where $i_1, i_2, \ldots, i_t \in (0,1,\ldots,n-1)$, and let their exponents be $r_1, r_2, \ldots, r_t$ respectively. The conjugacy class $C_{p,n}(i_s)$, $1 \leq s \leq t$, can take values from an ideal of $GR(p^k, r_s)$. For a given cyclic code L, let $C_{p,n}(i_s)$ take values from the ideal $p^{j_s}GR(p^k, r_s)$ where $0 \leq j_s \leq k$. The number of distinct values a DFT coefficient in $C_{p,n}(i_s)$ can assume is the number of elements in $p^{j_s}GR(p^k, r_s)$ which is equal to $p^{r_s(k-j_s)}$. Hence the total number of ways all the conjugacy classes can be assigned values is

$$p^{r_1(k-j_1)} p^{r_2(k-j_2)} \ldots\ldots p^{r_t(k-j_t)} = p^{\left(\sum_{s=1}^{t} r_s (k-j_s)\right)}$$

Hence for the cyclic code L, given by

$$L \equiv \bigotimes_{i=1}^{t} p^{j_i} GR(p^k, r_i)$$

the word-length μ is given by

$$\mu = \sum_{s=1}^{t} r_s(k-j_s)$$

and the number of codewords, denoted by M, is given by

$$M = p^{\mu} = p^{\left(\sum_{s=1}^{t} r_s(k-j_s)\right)} .$$

The formula obtained for μ is the generalisation of the result for the case of cyclic codes over finite fields which states that the dimension of a code over finite field is the number of nonzero spectral components in its transform domain description [14,15]. In the case of finite fields, k = 1 and j_i = 0 or 1, i.e, $p^{j_i} = 1$ or p. $p^{j_i} = 1$ corresponds to nonzero spectral components and $p^{j_i}=p$ corresponds to zero spectral components. So we have

$$\mu = \sum_{i=1}^{t} r_s(1-j_s) \qquad j_s = 0 \text{ or } j_s = 1$$

= sum of the exponents of the conjugacy classes which take nonzero values since for zero spectral components j_s =1.

= number of nonzero spectral components

= dimension of the code

Hence in the case of finite fields μ reduces to the dimension of the code.

Example 4.4 In this example, cyclic codes of length 3 over Z_4 are considered. The codewords of all cyclic codes have been given in Example 4.2. The wordlengths and number of codewords of all cyclic codes are listed in Table 4.5.

Example 4.5 We consider length 3 cyclic codes over Z_8 in this example. A complete listing of codewords of all cyclic codes can be found in Appendix A corresponding to Example 4.3. Word-lengths and number of codewords of all the codes is listed in Table 4.6.

4.2 SPECTRAL CHARACTERISATION FOR ARBITRARY m

In this section we extend the transform domain characterisation to cyclic codes over Z_m for any arbitrary value of m. In Subsection 4.2.1 a DFT suitable for cyclic codes over Z_m, $m=p_1^{k_1}p_2^{k_2},\ldots,p_s^{k_s}$, is described. In Subsection 4.2.2 spectral characterisation of cyclic codes over Z_m is obtained. It is shown that every cyclic code over Z_m is a direct product of cyclic codes over $Z_{p_i^{k_i}}$, $i=1,2,\ldots,s$.

4.2.1 DFT for the case $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$

Let $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$. To start with, our aim is to obtain an extension ring of Z_m which supports a DFT of length n. We proceed as follows:

Table 4.5 Listing of word-lengths and number of codewords of all length 3 cyclic codes over Z_4.

Any code, in this case, is of the form

$$\bigoplus_{i=1}^{2} 2^{j_i}GR(4,r_i)$$

i.e., $2^{j_1}GR(4,1) \oplus 2^{j_2}GR(4,2)$ for $j_1, j_2 = 0,1,2$.

The conjugacy classes are $C_{2,3}(0) = (0)$ and $C_{2,3}(1) = (1,2)$.

The exponents are $r_1 = 1$ and $r_2 = 2$.

For different values of j_1 and j_2, word-length μ and number of codewords M are listed below.

code	j_1	j_2	word-length μ $r_1(2-j_1)+r_2(2-j_2)$	number of codewords $M = 2^{\mu}$
N1	2	2	0	1
N2	2	1	2	4
N3	2	0	4	16
N4	1	2	1	2
N5	1	1	3	8
N6	1	0	5	32
N7	0	2	2	4
N8	0	1	4	16
N9	0	0	6	64

Table 4.6 Listing of word-lengths and number of codewords of all length 3 cyclic codes over Z_8.

Any code in this case is of the form

$$\bigoplus_{i=1}^{2} 2^{j_i} GR(8, r_i)$$

i.e., $2^{j_1}GR(8,1) \oplus 2^{j_2}GR(8,2)$ for $j_1, j_2 = 0,1,2,3$.

The conjugacy classes are $C_{2,3}(0) = \{0\}$ and $C_{2,3}(1) = (1,2)$.

The exponents are $r_1 = 1$ and $r_2 = 2$.

For different values of j_1 and j_2, word-length μ and the number of codewords M are listed below.

code	j_1	j_2	word-length $\mu = r_1(3-j_1)+r_2(3-j_2)$	number of codewords $M = 2^{\mu}$
N1	3	3	0	1
N2	3	2	2	4
N3	3	1	4	16
N4	3	0	6	64
N5	2	3	1	2
N6	2	2	3	8
N7	2	1	5	32
N8	2	0	7	128
N9	1	3	2	4
N10	1	2	4	16
N11	1	1	6	64
N12	1	0	8	256
N13	0	3	3	8
N14	0	2	5	32
N15	0	1	7	128
N16	0	0	9	512

Define m_i such that $m_i \equiv 1 \pmod{p_i^{k_i}}$ and $m_i \equiv 0 \pmod{p_j^{k_j}}$ for $i \neq j$, $i=1,2,\ldots,s$. Let $\emptyset_i(x)$ be a monic irreducible polynomial of degree r over Z_{p_i} and hence over $Z_{p_i^{k_i}}$, where r is the least integer such that $n \mid \gcd((p_1^r-1)(p_2^r-1)\ldots(p_s^r-1))$. Then $\emptyset(x)$, given by

$$\emptyset(x) = (m_1\emptyset_1(x) + m_2\emptyset_2(x) + \ldots + m_s\emptyset_s(x)) \bmod m$$

is a monic irreducible polynomial over Z_m of degree r [12] and define

$$Q(m,r) = Z_m[x]/\emptyset(x).$$

$Q(m,r)$ is the required extension ring of Z_m. It may be noted that

$$GR(p_i^{k_i},r) = Z_{p_i^{k_i}}[x]/\emptyset_i(x) \; ; \qquad i=1,2,\ldots,s.$$

<u>Lemma 4.1</u> $Q(m,r) \equiv \bigoplus_{i=1}^{s} GR(p_i^{k_i},r)$ and $Q^*(m,r) \equiv \bigotimes_{i=1}^{s} GR^*(p_i^{k_i},r)$.

<u>Proof:</u> $Q^*(m,r) \equiv \underset{i=1}{\overset{s}{\times}} GR^*(p_i^{k_i},r)$ has been proved in [12,Lemma 2], and $Q(m,r) \equiv \bigoplus_{i=1}^{s} GR(p_i^{k_i},r)$ can be proved in a similar way. Q.E.D.

From lemma 4.1 it is seen that the group of units of $Q(m,r)$ has order $N = \prod_{i=1}^{s} p_i^{r_i(k_i-1)}(p_i^r-1)$. Since $(n,m)=1$, we have $(n,p_i)=1$, $i=1,2,\ldots,s$ and we can choose r such that n divides the g.c.d. of $((p_1^r-1),(p_2^r-1),\ldots,(p_s^r-1))$ in which case $n \mid N$, and we can find an element $\alpha \in Q^*(m,r)$ of order n. Hence for an n-tuple $(a_0,a_1,\ldots,a_{n-1}) \in Z_m^n$, the transform vector $(A_0,A_1,..,A_{n-1}) \in Q^n(m,r)$ is given by

$$A_j = \sum_{i=0}^{n-1} \alpha^{ij} a_i, \qquad j=0,1,\ldots,n-1.$$

4.2.2 Spectral characterisation

As in the case of $m = p^k$, our next step is to identify the subring R_T of $Q^n(m,r)$ which is the image of all n-tuples over Z_m under DFT. This requires the knowledge of the group of automorphisms of $Q(m,r)$.

The group of automorphisms of $Q(m,r)$ is an abelian group which is direct product of s cyclic groups each of order r. Let $\sigma_1,\sigma_2,\ldots,\sigma_s$ be the generator automorphisms of these cyclic groups. Then σ_i, $i=1,2,\ldots,s$, is the generator of the group of automorphisms of $GR(p_i^{k_i},r)$ [30]. Clearly any map $\sigma:Q(m,r) \longrightarrow Q(m,r)$ of the form $(\sigma_1^{j_1},\sigma_2^{j_2},\ldots,\sigma_s^{j_s})$ is an automorphism and conversely. It is to be noted that each generating automorphism relates different set of spectral components of conjugacy classes corresponding to different p_i. Let $(A_0,A_1,\ldots,A_{n-1})$ be a transform vector where $A_i \in Q(m,r)$ and A_{ij} is the component of A_i in $GR(p_j^{k_j},r)$ under the isomorphism

$$Q(m,r) \equiv \bigoplus_{i=1}^{s} GR(p_i^{k_i},r).$$

Then from conjugacy symmetry property we have $\sigma_j(A_{ij}) = A_{i(pj)}$. Let there be t_i conjugacy classes corresponding to p_i with exponents e_{ij}, $j=1,2,\ldots,t_i$, for $i=1,2,\ldots,s$. The following theorem identifies the subring R_T of $Q^n(m,r)$.

Theorem 4.4: The subring R_T of $Q_s^n(m,r)$ which contains all the transform vectors of n-tuples over Z_m, $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, is

isomorphic to $\bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GR(p_i^{k_i}, e_{ij})$ where t_i is the number of conjugacy classes and e_{ij}, $j=1,2,\ldots,t_i$, are the exponents corresponding to p_i.

Proof: Let $(a_0,a_1,\ldots,a_{n-1}) \in Z_m^n$ and let $(A_0,A_1,\ldots,A_{n-1}) \in Q^n(m,r)$ be its transform vector. Let us take a fixed component of the transform vector say A_j. Since

$$A_j \in Q(m,r) \equiv \bigoplus_{i=1}^{s} GR(p_i^{k_i},r),$$

it follows that $A_j = (A_{j_1},A_{j_2},\ldots,A_{j_s})$ where $A_{j_q} \in GR(p_q^{k_q},r)$ for $q=1,2,\ldots,s$. Let $\exp_p(j) = e_{qh}$ where $h \in (1,2,\ldots,t_q)$. From Theorem 4.1, it follows that $A_{j_q} \in GR(p_q^{k_q},e_{qh})$. Considering all other components of A_j and for all $j = 0,1,2,..,(n-1)$, we have

$$R_T \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GR(p_i^{k_i},e_{ij}). \qquad \text{Q.E.D.}$$

From Theorem 4.4, we have

$$Z_m[x]/(x^n-1) \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GR(p_i^{k_i},e_{ij})$$

Hence any cyclic code L over Z_m, i.e., ideal of $Z_m[x]/(x^n-1)$, is of the form

$$L \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} p^{h_{ij}} GR(p_i^{k_i},e_{ij}) \quad ; \quad 0 \le h_{ij} \le k_i. \qquad (4.2)$$

It is to be noted that in the above isomorphism the first isomorphism is over different primes which is due to the Chinese

remainder theorem whereas the second isomorphism arises due to the disjointness of the conjugacy classes for a given prime and n. It is also to be noted that the conjugacy class structure for two primes need not be same for a given n. In the next section we obtain Theorem 4.10 that gives condition under which two primes give rise to identical conjugacy class structure for a given n.

By choosing zero ideal from all $GR(p_i^{k_i}, e_{ij})$ except, say, i=u, in (4.2) we obtain a cyclic code over $Z_{p_u^{k_u}}$, given by

$$L_u = \bigoplus_{j=1}^{t_u} p^{h_{ij}} GR(p_u^{k_u}, e_{ij}) \; ; \quad 0 \le h_{ij} \le k_i .$$

This implies that every cyclic code over Z_m, $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, is a direct sum of codes over $Z_{p_i^{k_i}}$, i=1,2,...,s. This fact is stated in the following theorem.

Theorem 4.5: Every cyclic code over Z_m, $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, is a direct sum of cyclic codes over $Z_{p_i^{k_i}}$, i=1,2,...,s.

Example 4.6 Let $m=12=3.2^2$ and n=5. The appropriate extension ring is $Z_{12}[x]/(x^4+x+1) \equiv GR(4,4) \oplus GR(3,4)$. Conjugacy classes are $C_{2,5}(0) = \{0\}$, $C_{2,5}(1) = \{1,2,3,4\}$, $C_{3,5}(0) = \{0\}$ and $C_{3,5}(1) = \{1,2,3,4\}$. From Theorem 4.4, it follows that

$$Z_{12}[x]/(x^4+x+1) \equiv GR(4,1) \oplus GR(4,4) \oplus GR(3,1) \oplus GR(3,4)$$
$$\equiv Z_4 \oplus GR(4,4) \oplus GF(3) \oplus GF(3^4)$$

Conjugacy class (0) can take ideals of $Z_4 \oplus GF(3)$ and conjugacy

class (1,2,4,3) can take ideals of GR(4,4) $\oplus$ GF(3^4). Let us take the ideal GF(3) for the conjugacy class (0) and 2GR(4,4) for the conjugacy class (1,2,4,3). In $Z_{12}[x]/(x^4+x+1)$ the subring isomorphic to GF(3) is (0000,4000,8000) and the subring isomorphic to 2GR(4,4) is all the entries listed in the spectral component A_1 of Table 4.7 in the next page, which lists all the codewords with their spectrum.

Theorem 4.6: The minimum Hamming distance of a code L over Z_m, where

$$L \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} p^{h_{ij}} GR(p_i^{k_i}, e_{ij}) \; ; \quad 0 \leq h_{ij} \leq k_i,$$

is equal to the minimum of the minimum Hamming distances of the codes L_i, i=1,2,...,s, over $Z_{p_i^{k_i}}$, given by

$$L_i \equiv \bigoplus_{j=1}^{t_i} p^{h_{ij}} GR(p_i^{k_i}, e_{ij}).$$

Proof: Let d be the minimum Hamming distance of L and d_i, i=1,2,...,s, be the minimum Hamming distances of L_i, i=1,2,...,s. Let $d_v = \min(d_1, d_2, \ldots, d_s)$ for some $v \in \{1,2,\ldots s\}$. We have

$$L \equiv \bigoplus_{i=1}^{s} L_i \; .$$

By choosing the zero vector from all L_i, except i = v, and a vector of Hamming weight d_v in L_v, we obtain a codeword in L of Hamming weight d_v in L. Hence $d \leq d_v$. We want to show that $d = d_v$.

Table 4.7 Codewords and spectrum corresponding to Example 4.6.

codewords					spectrum				
a_0	a_1	a_2	a_3	a_4	A_0	A_1	A_2	A_3	A_4
0	0	0	0	0	0000	0000	0000	0000	0000
6	6	0	0	0	0000	6066	0666	6006	6606
0	6	6	0	0	0000	6600	6060	0060	0600
0	6	0	6	0	0000	0060	6600	0600	6060
6	6	6	6	0	0000	0606	0006	6666	0066
2	8	2	2	2	4000	0066	6666	0006	0606
8	8	2	8	2	4000	6060	0600	6600	0060
2	8	8	8	2	4000	6606	6006	0666	6066
10	10	4	4	4	8000	6066	0666	6006	6606
4	10	10	4	4	8000	6600	6060	0060	0600
4	10	4	10	4	8000	0060	6600	0600	6060
10	10	10	10	4	8000	0606	0006	6666	0066
0	6	0	0	6	0000	0660	6660	6660	0660
6	6	6	0	6	0000	0006	0066	0606	6666
6	6	0	6	6	0000	6666	0606	0066	0006
0	6	6	6	6	0000	6000	6000	6000	6000
8	8	2	2	8	4000	6660	0660	0660	6660
2	8	8	2	8	4000	6006	6066	6606	0666
2	8	2	8	8	4000	0666	0606	6066	6006
8	8	8	8	8	4000	0000	0000	0000	0000
4	10	4	4	10	8000	0660	6660	6660	0660
10	10	10	4	10	8000	0006	0066	0606	6666
10	10	4	10	10	8000	6666	0606	0066	0006
4	10	10	10	10	8000	6000	6000	6000	6000
6	0	6	0	0	0000	0666	6606	6066	6006
6	0	0	6	0	0000	6006	6066	6606	0666
0	0	6	6	0	0000	6660	0660	0660	6660
8	2	2	2	2	4000	6000	6000	6000	6000
2	2	8	2	2	4000	6666	0606	0066	0006
2	2	2	8	2	4000	0006	0066	0606	6066
8	2	8	8	2	4000	0660	6660	6660	0660
4	4	4	4	4	8000	0000	0000	0000	0000
10	4	10	4	4	8000	0666	6606	6066	6006
10	4	4	10	4	8000	6006	6066	6606	0666
4	4	10	10	4	8000	6660	0660	0660	6660
6	0	0	0	6	0000	6006	6006	0666	6066
0	0	6	0	6	0000	6060	0600	6600	0060
0	0	0	6	6	0000	0600	0060	6060	6600
6	0	6	6	6	0000	0066	6666	6006	0606
2	2	2	2	8	4000	0606	0006	6666	0066
8	2	8	2	8	4000	0060	6600	0600	6060
8	2	2	8	8	4000	6600	6060	0060	0600
2	2	8	8	8	4000	6066	0666	6006	6606
10	4	4	4	10	8000	6606	6006	0666	6066
4	4	10	4	10	8000	6060	0600	6600	0060
4	4	4	10	10	8000	0600	0060	6060	6600
10	4	10	10	10	8000	0066	6666	0006	0606

Suppose $d < d_v$. Let Γ be a codeword in L of Hamming weight d. i.e., there are only d nonzero components in Γ which are elements of Z_m. In the isomorphism $Z_m \equiv \bigoplus_{i=1}^{s} Z_{p_i^{k_i}}$, the zero of Z_m has only zero components in all $Z_{p_i^{k_i}}$, and any non-zero element of Z_m has nonzero component in at least one $Z_{p_i^{k_i}}$. Hence if Γ_i, $i=1,2,\ldots,s$ are components of Γ in L_i, $i=1,2,\ldots,s$, then Hamming weight of each L_i is atmost d. This means the minimum Hamming weight of L_i is equal to $d < d_v$ for at least one i, which contradicts the minimality of d_v. Hence $d = d_v$. Q.E.D.

From the formula obtained for μ in Subsection 4.1.5, it follows that the number of codewords in L can be shown to be equal to $\prod_{i=1}^{s} p_i^{\mu_i}$, where μ_i is the word-length of the cyclic code L_i.

4.3 SPECTRAL CHARACTERISATION FOR $m = p_1p_2\ldots p_s$

In this section the special case of m being equal to a product of distinct primes, $m=p_1p_2\ldots.p_s$, is considered. It is seen that in this case every cyclic code over Z_m is a direct sum of cyclic codes over finite fields $GF(p_i)$, $i=1,2,\ldots,s$. In this case, Z_m is a semisimple ring and by Masche's theorem the ring $Z_m[x]/(x^n-1)$ is also semisimple. Hence every cyclic code over Z_m has an idempotent generator. In Subsection 4.3.1, it is proved that the transform vectors of these idempotent generators can be identified in a simple way, in terms of idempotent elements of Z_m. In Subsection 4.3.2, the question of when does two primes p_1

and p_2, for a given n, give rise to identical conjugacy class structure is discussed.

4.3.1 Idempotent generators

Proceeding as in the previous section and using the facts

$$GR(p,r) \equiv GF(p^r) \quad \text{and} \quad Q(m,r) \equiv \bigoplus_{i=1}^{s} GF(p_i^r),$$

we have

$$Q^*(m,r) \equiv \bigtimes_{i=1}^{s} GF^*(p_i^r) .$$

Putting $k_1 = k_2 = \ldots = k_s = 1$ in Theorem 4.4, we obtain

Theorem 4.7 The subring R_T of $Q^n(m,r)$ which contains all the transform vectors of n-tuples over Z_m, $m = p_1p_2\ldots p_s$, is isomorphic to $\bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GF(p_i^{e_{ij}})$, where t_i is the number of conjugacy classes corresponding to p_i and e_{ij}, $j=1,2,\ldots,t_i$, are their exponents.

From Theorem 4.4 it follows that

$$Z_m[x]/(x^n-1) \equiv R_T \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GF(p_i^{e_{ij}})$$

i.e., $Z_m[x]/(x^n-1)$ is a direct sum of finite fields $GF(p_i^{e_{ij}})$, $i=1,2,\ldots,s$ and $j=1,2,\ldots,t_i$. Hence every cyclic code over Z_m, which is an ideal of $Z_m[x]/(x^n-1)$, has an idempotent generator.

Example 4.7: Let m=6 and n=5. Z_6 is isomorphic to the direct sum of Galois fields GF(2) and GF(3). $\emptyset_1(x)$ and $\emptyset_2(x)$, irreducible polynomials of degree 4 over GF(2) and GF(3), are given by $\emptyset_1(x) = x^4+x+1$ and $\emptyset_2(x) = x^4+x+2$. $\emptyset(x)$, irreducible polynomial of degree 4 over Z_6 is x^4+x+5. We have

$$Q(6,4) = Z_6[x]/(x^4+x+5).$$

In Q(6,4) an element of order 5 is $2x^2+3x^3$. This element is taken to be the transform factor. The resulting DFT matrix is given below. An element $a+bx+cx^2+dx^3$ of Q(6,4) is denoted by abcd.

$$\begin{bmatrix} 1000 & 1000 & 1000 & 1000 & 1000 \\ 1000 & 0023 & 2435 & 4123 & 5151 \\ 1000 & 2435 & 5151 & 0023 & 4123 \\ 1000 & 4123 & 0023 & 5151 & 2435 \\ 1000 & 5151 & 4123 & 2435 & 0023 \end{bmatrix}$$

The conjugacy classes are $C_{2,5}(0) = \{ 0 \}$, $C_{2,5}(1) = \{1,2,3,4 \}$, $C_{3,5}(0) = \{ 0 \}$ and $C_{3,5}(1) = \{ 1,2,3,4 \}$. We have

$$Z_6[x]/(x^5-1) \equiv GF(2) \oplus GF(2^4) \oplus GF(3) \oplus GF(3^4)$$

We take zero ideal for the conjugacy classes $C_{2,5}(0)$ and $C_{3,5}(1)$ and full ring for the conjugacy classes $C_{3,5}(0)$ and $C_{2,5}(1)$. The codewords and their transform vectors of the resulting code is listed in Table 4.8 in the next page.

Table 4.8 Codewords and spectrum of the code of Example 4.7.

codewords					spectrum				
a_0	a_1	a_2	a_3	a_4	A_0	A_1	A_2	A_3	A_4
0	0	0	0	0	0000	0000	0000	0000	0000
3	3	0	0	0	0000	3003	3033	3303	0333
3	0	0	3	0	0000	3303	3003	0333	3033
3	3	3	3	0	0000	3333	0303	0033	0003
1	1	4	1	1	2000	0033	3333	0003	0303
4	4	1	4	1	2000	3300	3030	0030	0300
2	2	2	2	2	4000	0000	0000	0000	0000
2	5	5	2	2	4000	0030	3300	0300	3030
2	2	5	5	2	4000	0330	3330	3330	0330
0	3	0	0	3	0000	3330	0330	0330	3330
0	0	0	3	3	0000	3030	0300	3300	0030
0	3	3	3	3	0000	3000	3000	3000	3000
4	1	4	1	4	2000	0300	0030	3030	3300
1	4	1	4	4	2000	3033	0333	3003	3303
5	2	2	2	5	4000	0333	3303	3033	3003
5	5	5	2	5	4000	0303	0003	3333	0033
5	2	5	5	5	4000	0003	0033	0303	3333
3	0	3	0	0	0000	3033	0333	3003	3303
0	3	0	3	0	0000	0300	0030	3030	3300
4	1	1	1	1	2000	3000	3000	3000	3000
4	4	4	1	1	2000	3030	0300	3300	0030
4	1	4	4	1	2000	3330	0330	0330	3330
5	5	2	2	2	4000	3003	3033	3303	0333
5	2	2	5	2	4000	3303	3003	0333	3033
5	5	5	5	2	4000	3333	0303	0033	0003
0	0	3	0	3	0000	3300	3030	0030	0300
3	3	0	3	3	0000	0033	3333	0003	0303
1	1	1	1	4	2000	3333	0303	0033	0003
1	4	4	1	4	2000	3303	3003	0333	3033
1	1	4	4	4	2000	3003	3033	3303	0333
2	5	2	2	5	4000	3330	0330	0330	3330
2	2	2	5	5	4000	3030	0300	3300	0030
2	5	5	5	5	4000	3000	3000	3000	3000
0	3	3	0	0	0000	0030	3300	0300	3030
0	0	3	3	0	0000	0330	3330	3330	0330
1	4	1	1	1	2000	0003	0033	0303	3333
1	1	1	4	1	2000	0303	0003	3333	0033
1	4	4	4	1	2000	0333	3303	3033	3003
5	2	5	2	2	4000	3033	0333	3003	3303
2	5	2	5	2	4000	0300	0030	3030	3300
3	0	0	0	3	0000	0333	3303	3033	3003
3	3	3	0	3	0000	0303	0003	3333	0033
3	0	3	3	3	0000	0003	0033	0303	3333
4	4	1	1	4	2000	0330	3330	3330	0330
4	1	1	4	4	2000	0030	3300	0300	3030
4	4	4	4	4	2000	0000	0000	0000	0000
2	2	5	2	5	4000	3300	3030	0030	0300
5	5	2	5	5	4000	0033	3333	0003	0303

Theorem 4.8 All the idempotent generator polynomials of ideals of $Q(m,r)$ have degree zero and hence correspond to idempotent elements of Z_m. i.e., if $a_0+a_1x+\ldots+a_{r-1}x^{r-1} \in Q(m,r)$ is a generator of some ideal of $Q(m,r)$ then $a_1 = a_2 = \ldots = a_{r-1} = 0$ and a_0 is an idempotent element of Z_m.

Proof: Let I be an ideal of $Q(m,r)$ with idempotent generator e. From $Q(m,r) \equiv \bigoplus_{i=1}^{s} GF(p_i^r)$, it follows that $I \equiv \bigoplus_{i=1}^{s} I_i$, where I_i is an ideal in $GF(p_i^r)$ and $e = (m_1e_1+m_2e_2+\ldots+m_se_s) \bmod m$, where e_i is an idempotent generator of I_i. In a finite field there are only two ideals generated by 0 and 1 both having degree zero. Hence the degree of e must be zero which means e is an idempotent element of Z_m. Q.E.D.

Theorem 4.9 Every cyclic code over Z_m, $m = p_1p_2\ldots p_s$, is uniquely determined by a subset of idempotent elements of Z_m.

Proof: Every cyclic code over Z_m, $m=p_1p_2\ldots.p_s$, has an idempotent generator. Let $(f_0,f_1,\ldots,f_{n-1})$ be an idempotent generator of a cyclic code with $(F_0,F_1,\ldots,F_{n-1})$ as its transform vector. Since the conjugacy constraints corresponding to a prime p_j, $j=1,2,\ldots,s$, is of the form $F_i = F_{p_j i}$, $i=0,1,2,\ldots(n-1)$, from Theorem 4.8, it follows that $F_i \in Z_m$, for $i=0,1,2,\ldots,(n-1)$. Moreover, the group of automorphisms of $Q(m,r)$ leave the subring Z_m invariant. This means if j-th component of transform vector is $F_j \in Z_m$ then all the spectral components of the conjugacy class $C_{p,n}(j)$ take the value F_j. Hence idempotent generators can be identified in the transform domain as those which have some idempotent elements of Z_m in all the conjugacy classes. Q.E.D.

Example 4.8 : Consider length 5 cyclic codes over Z_6. The conjugacy classes are $C_{2,5}(0) = \{ 0 \}$, $C_{2,5}(1) = \{ 1,2,3,4 \}$, $C_{3,5}(0) = \{ 0 \}$ and $C_{3,5}(1) = \{ 1,2,3,4 \}$. The idempotent elements of Z_6 are 0,1,3 and 4. The idempotent generators of all cyclic codes and their spectrum are listed in Table 4.9.

Example 4.9: Let n=7 and m=6=2x3. The conjugacy classes are $C_{2,7}(0) = \{ 0 \}$, $C_{2,7}(1) = \{ 1,2,4 \}$, $C_{2,7}(3) = \{ 3,6,5 \}$, $C_{3,7}(0) = \{ 0 \}$ and $C_{3,7}(1) = \{ 1,2,3,4,5,6 \}$ and their exponents respectively are 1, 3, 3, 1 and 6. The appropriate extension ring is Q(6,6). All the cyclic codes are ideals of

$$Z_6[x]/(x^7-1) \equiv GR(2,1) \oplus GR(2,3) \oplus GR(2,3) \oplus GR(3,1) \oplus GR(3,6)$$

The idempotent elements of Z_6 are 0,1,3 and 4. We can straight away write the transform vectors of idempotent generators as listed in Table 4.10.

Theorem 4.11: The number of nontrivial cyclic codes of length n over Z_m where $m = p_1 p_2 \ldots p_s$ is given by $\prod_{i=1}^{s} (2^{t_i})-2$, where t_i is the number of conjugacy classes for n corresponding to p_i.

Proof: From Theorem 4.7, it follows that

$$Z_m[x]/(x^n-1) \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GF(p_i^{e_{ij}}).$$

For a fixed $i \in (1,2,\ldots,s)$ there are t_i conjugacy classes. Each conjugacy class can assume either 0 or 1 of $GF(p_i^{e_{ij}})$ from Theorem 4.6, So there are 2^{t_i} idempotent generators corresponding to p_i. Varying i through (1,2,...,s), we get 2^{t_i} codes. Hence there are $(2^{t_i})-2$ cyclic codes corresponding to p_i. Since there

Table 4.9 Listing of idempotent generators of all cyclic codes of length 5 over Z_6.

e_0	e_1	e_2	e_3	e_4	E_0	E_1	E_2	E_3	E_4
0	0	0	0	0	0000	0000	0000	0000	0000
1	0	0	0	0	1000	1000	1000	1000	1000
3	0	0	0	0	3000	3000	3000	3000	3000
4	0	0	0	0	4000	4000	4000	4000	4000
2	1	1	1	1	0000	1000	1000	1000	1000
5	1	1	1	1	3000	4000	4000	4000	4000
2	2	2	2	2	4000	0000	0000	0000	0000
5	2	2	2	2	1000	3000	3000	3000	3000
0	3	3	3	3	0000	3000	3000	3000	3000
1	3	3	3	3	1000	4000	4000	4000	4000
3	3	3	3	3	3000	0000	0000	0000	0000
4	3	3	3	3	4000	1000	1000	1000	1000
2	4	4	4	4	0000	4000	4000	4000	4000
5	4	4	4	4	3000	1000	1000	1000	1000
2	5	5	5	5	4000	3000	3000	3000	3000
5	5	5	5	5	1000	0000	0000	0000	0000

Table 4.10 Listing of idempotent generators in the transform domain of all cyclic codes of length 7 over Z_6.

E_0	E_1	E_2	E_3	E_4	E_5	E_6
000000	000000	000000	000000	000000	000000	000000
300000	300000	300000	300000	300000	300000	300000
300000	000000	000000	300000	000000	300000	300000
000000	300000	300000	000000	300000	000000	000000
300000	300000	300000	000000	300000	000000	000000
000000	300000	300000	300000	300000	300000	300000
000000	000000	000000	300000	000000	300000	300000
300000	000000	000000	000000	000000	000000	000000
100000	300000	300000	000000	300000	000000	000000
100000	000000	000000	300000	000000	300000	300000
400000	300000	300000	000000	300000	000000	000000
400000	000000	000000	300000	000000	300000	300000
400000	300000	300000	300000	300000	300000	300000
100000	300000	300000	300000	300000	300000	300000
400000	000000	000000	000000	000000	000000	000000
100000	000000	000000	000000	000000	000000	000000
400000	100000	100000	400000	100000	400000	400000
400000	400000	400000	400000	400000	400000	400000
100000	100000	100000	100000	100000	100000	100000
100000	400000	400000	100000	400000	100000	100000
100000	400000	400000	400000	400000	400000	400000
400000	400000	400000	100000	400000	100000	100000
000000	100000	100000	400000	100000	400000	400000
000000	400000	400000	400000	400000	400000	400000
100000	100000	100000	400000	100000	400000	400000
400000	100000	100000	100000	100000	100000	100000
000000	100000	100000	100000	100000	100000	100000
300000	100000	100000	400000	100000	400000	400000
300000	400000	400000	400000	400000	400000	400000
300000	100000	100000	100000	100000	100000	100000
000000	400000	400000	100000	400000	100000	100000
300000	400000	400000	100000	400000	100000	100000

are s primes the total number of nontrivial cyclic codes possible, taking direct sum, is $\prod_{i=1}^{s} (2^{t_i})-2$. Q.E.D.

When s = 1, m is a prime number p and $Z_m \equiv GF(p)$, our codes become codes over a finite field.

In [31] it is shown that some special case of codes over Z_m, $m = p_1 p_2 \ldots p_s$, can be used to implement an efficient coding scheme for the multiaccess communication system where the efficiency is in terms of information rate.

4.3.2 Identical conjugacy class structure for distinct primes

In Chapter 2 it was seen that for a given n and two primes p_1 and p_2, both relatively prime to n, there will be identical conjugacy structure if p1 = p2 (mod n). In this subsection we identify another condition under which identical conjugacy class structure is obtained when $p_1 \neq p_2$ (mod n).

In Example 4.8 and Example 4.9, both over Z_6, the idempotent elements of Z_6 are 0,1,3 and 4. In Example 4.8 the conjugacy classes for different primes i.e., 2 and 3, are identical. Whereas in Example 4.9 the conjugacy classes corresponding to two primes 2 and 3 are different. In writing the transform vectors of idempotent generators this has to be taken into account. It can be seen that in Example 4.9 the conjugacy class (0) takes all the

idempotents whereas the conjugacy classes (1,2,4) and (3,5,6) are constrained in taking idempotent elements. For instance the transform vector $(E_0\ E_1\ E_2\ E_3\ E_4\ E_5\ E_6)$
= (* 300000 300000 400000 300000 400000 400000) or
= (* 300000 300000 100000 300000 100000 100000),
where * for E_0 being any idempotent element, does not appear in the listing of idempotent generators, though 1, 3, and 4 are idempotent elements of Z_m. Such a constraint is not there in Example 4.8. This is due to the fact that the conjugacy classes for given n corresponding to different primes in m give different conjugacy class structure. We give below a theorem which gives the pairs of primes that will give identical conjugacy class structure for given n.

Theorem 4.10: For a given n and a prime p_1 relatively prime to n, let $\exp_n(p_1) = e$. If p_2 is a prime such that $p_1^a = p_2 \pmod n$ for some integer a with (a,e) = 1, then $C_{p_1,n}(j) = C_{p_2,n}(j)$ for all j. i.e., p_1 and p_2 give identical conjugacy class structure.

Proof: Consider the sets (all elements considered modulo n)

$$S1 = (1,\ p_2,\ p_2^2,\ p_2^3,\ \ldots,\ p_2^{e-2},\ p_2^{e-1}) \qquad (4.3.1)$$

and
$$S2 = (1,\ p_1,\ p_1^2,\ p_1^3,\ \ldots,\ p_1^{e-2},\ p_1^{e-1}). \qquad (4.3.2)$$

Since $p_1^a = p_2 \pmod n$ the set S1 can be written as

$$S3 = (1,\ p_1^a,\ p_1^{2a},\ \ldots\ldots,\ p_1^{a(e-2)},\ p_1^{a(e-1)}). \qquad (4.3.3)$$

Since (a,e) = 1, sets S2 and s3 are same and hence sets S1 and S2. Moreover, $p_2^e = p_1^{ae} = 1 \pmod n$. Hence

$$\exp_n(p_2) = e. \qquad (4.3.4)$$

Our aim is to prove that $C_{p_1,n}(j) = C_{p_2,n}(j)$ for $j \in (0,1,..,n-1)$

Let $j \in (0,1,\ldots,(n-1))$.

If (j,n) = 1, then

$$C_{p_1,n}(j) = (j, jp_1, jp_1^2, \ldots, jp_1^{(e-1)}) \qquad (4.3.5)$$

$$C_{p_2,n}(j) = (j, jp_2, jp_2^2, \ldots, jp_2^{(e-1)}). \qquad (4.3.6)$$

Multiplying the elements of sets S1 and S2 by j, we obtain (4.3.5) and (4.3.6). Since S1 and S2 are same and (j,n)=1, the sets given in (4.3.5) and (4.3.6) are same.

i.e., $C_{p_1 n}(j) = C_{p_2 n}(j)$ if(j,n)=1.

If (j,n) ≠ 1, then let (j,n) = d.

We have $(jp_1^k) \pmod n = (j/d)p_1^k \bmod(n/d)$ for any integer k.

Putting j/d = j' and n/d = q, we

obtain $$jp_1^k \pmod n = j'p_1^k \pmod q. \qquad (4.3.7)$$

q is a divisor of n. Let $\exp_q(p_1) = e'$. i.e., $q \mid (p_1^{e'} - 1)$. Since $\exp_n(p_1) = e$, we have $n \mid p_1^e - 1$. From $q \mid n$, it follows that $p_1^{e'} - 1 \mid p_1^e - 1$ which means $e' \mid e$. Also (a,e')=1 since (a,e)=1. Moreover, $p_1^a = p_2 \pmod n$, implies $p_1^a = p_2 \pmod q$. Hence

$$\exp_q(p_2) = e'. \qquad (4.3.8)$$

Since (j',q)=1, we have the sets (all elements considered mod q)

$$(j', j'(p_1), j'(p_1^2), \ldots, j'(p_1^{(e'-1)}))$$

and

$$(j', j'(p_2), j'(p_2^2), \ldots, j'(p_2^{(e'-1)})) \text{ same.}$$

Hence, from (4.3.7), $C_{p_1,n}(j) = C_{p_2,n}(j)$. Q.E.D.

Example 4.10: We list in Table 4.11 several cases where for a given n and two primes p_1 and p_2 ($p_1 \not\equiv p_2 \pmod n$) the conjugacy class structure.

4.4 BCH CODES OVER Zm

A BCH code over a finite field is defined as the cyclic code which has spectral zeros in consecutive spectral components [14,15]. BCH codes over finite fields form a subclass of cyclic codes over finite fields and the term 'consecutive zeros' instead of zeros in the spectral components defines this subclass. In the case of codes over Z_{p^k}, elements from a specified ideal of the extension ring define a cyclic code and naturally we define a BCH code over Z_{p^k} as the cyclic code with elements from the same ideal in consecutive spectral components.

BCH codes over Z_m have been studied by Prithi Shankar [12] in terms of generator polynomials. It is to be noted that in [12] BCH codes over Z_m are defined as the cyclic codes over Z_m whose

Table 4.11 Some identical conjugacy class structures

(1) n=5; $p_1 = 2(\text{mod } 5)$; $\exp_5(p_1) = 4$

$C_{p_1,5}(0) = \{0\}$, $C_{p_1,5}(1) = \{1,2,3,4\}$;

$p_2 = 3(\text{mod } 5)$; $\exp_5(p_2) = 4$

$C_{p_2,5}(0) = \{0\}$, $C_{p_2,5}(1) = \{1,2,3,4\}$;

Note that $2^3 = 3(\text{mod } 5)$ and $(3,4) = 1$.

(2) n=7; $p_1 = 2(\text{mod } 7)$; $\exp_7(p_1) = 3$

$C_{p_1,7}(0) = \{0\}$, $C_{p_1,7}(1) = \{1,2,4\}$,

$C_{p_1,7}(3) = \{3,5,6\}$

$p_2 = 4(\text{mod } 7)$; $\exp_7(p_2) = 3$

$C_{p_2,7}(0) = \{0\}$, $C_{p_2,7}(1) = \{1,2,4\}$,

$C_{p_2,7}(3) = \{3,5,6\}$.

Also $2^2 = 4(\text{mod } 7)$ and $(2,3) = 1$.

(3) n=7; $p_1 = 3(\text{mod } 7)$; $\exp_7(p_1) = 6$

$C_{p_1,7}(0) = \{0\}$, $C_{p_1,7}(1) = \{1,2,3,4,5,6\}$;

$p_2 = 5(\text{mod } 7)$; $\exp_7(p_2) = 6$

$C_{p_2,7}(0) = \{0\}$; $C_{p_2,7}(1) = \{1,2,3,4,5,6\}$;

We have $3^5 = 5(\text{mod } 7)$ with $(5,6) = 1$.

(4) n=15; $p_1 = 2(\text{mod } 15)$; $\exp_{15}(p_1) = 4$.

$C_{p_1,15}(0) = \{0\}$, $C_{p_1,15}(1) = \{1,2,4,8\}$,

$C_{p_1,15}(3) = \{3,6,9,12\}$, $C_{p_1,15}(7) = \{7,11,13,14\}$,

$C_{p_1,15}(5) = \{5,10\}$.

$p_2 = 8(\text{mod } 15)$; $\exp_{15}(p_2) = 4$.

$C_{p_2,15}(0) = \{0\}$, $C_{p_2,15}(1) = \{1,2,4,8\}$,

$C_{p_2,15}(5) = \{5,10\}$

$C_{p_2,15}(3) = \{3,6,9,12\}$, $C_{p_2,15}(7) = \{7,11,13,14\}$.

Also $2^3 = 8 \pmod{15}$ and $(3,4) = 1$.

(5) $n=15$; $p_1 = 7 \pmod{15}$; $\exp_{15}(p_1) = 4$.

$C_{p_1,15}(0) = \{0\}$, $C_{p_1,15}(1) = \{1,7,4,13\}$,

$C_{p_1,15}(3) = \{3,6,9,12\}$, $C_{p_1,15}(5) = \{5\}$,

$C_{p_1,15}(10) = \{10\}$, $C_{p_1,15}(2) = \{2,8,11,14\}$;

$p_2 = 13 \pmod{15}$; $\exp_{15}(p_2) = 4$

$C_{p_2,15}(0) = \{0\}$, $C_{p_2,15}(1) = \{1,7,4,13\}$,

$C_{p_2,15}(3) = \{3,6,9,12\}$, $C_{p_2,15}(5) = \{5\}$,

$C_{p_2,15}(10)=\{10\}$, $C_{p_2,15}(2) = \{2,8,11,14\}$;.

Also $7^3 = 13 \pmod{15}$ and $(3,4) = 1$.

For $n=15$ and $p = 4 \pmod{15}$ the conjugacy classes are $\{0\}$, $\{1,4\}$, $\{2,8\}$, $\{3,12\}$, $\{5\}$, $\{6,9\}$, $\{7,13\}$, $\{10\}$ and $\{14\}$. And $\exp_{15}(p) = 2$.

generator polynomial has consecutive roots of the form β^j, β^{j+1}, β^{j+2}, ...,$\beta^{j+(d-1)}$ in the extension ring where β is a generator of the cyclic subgroup of the group of units of the extension ring of order n (code length). In terms of spectral domain characterisation this is same as defining BCH codes as cyclic codes which have zeros in consecutive spectral components. Our definition of BCH codes over Z_m includes these as a subclass.

First we consider the case $m=p^k$.

Definition 4.5: A BCH code of length n over Z_{p^k} consists of the inverse DFT of all vectors whose d consecutive DFT coefficients are from the same ideal. In terms of conjugacy classes, the conjugacy classes which contain any one of the d consecutive spectral components take values from the specified ideal of the extension ring and other conjugacy classes take values from the full ring.

Let $C_{p,n}(j_1)$, $C_{p,n}(j_2)$,...,$C_{p,n}(j_s)$ be the conjugacy classes whose union contain the d consecutive spectral components and $r_1,r_2,...,r_s$ respectively be their exponents. The conjugacy class $C_{p,n}(j_i)$, i=1,2,...,s, takes values from an ideal of the Galois ring $GR(p^k,r_i)$, which is a subring of the extension ring $GR(p^k,r)$. Since all the conjugacy classes $C_{p,n}(j_i)$, i=1,2,...,s, are to take values from the same ideal of $GR(p^k,r)$, it is required that this ideal is contained in all the subrings

$GR(p^k,r_i)$, i=1,2,...s. Hence our choice of ideals for consecutive spectral components is restricted to the ideals of the subring $GR(p^k,r_g)$, where r_g is the g.c.d of $(r_1,r_2,\ldots,r_s)$. Specifically, the ideals from which the d consecutive spectral components can take values are all ideals of $GR(p^k,r_g)$, viz. $p^0GR(p^k,r_g)$, $p^1GR(p^k,r_g)$,.... ,$p^kGR(p^k,r_g)$. Note that $p^kGR(p^k,r_g)$ is the zero ideal and the BCH codes obtained when the consecutive spectral components take values from this ideal is precisely the BCH codes discussed by Prithi Shankar.

When the Hamming metric is considered, these BCH codes, except the ideal from which d consecutive spectral components take values are from zero ideal, have Hamming distance 1 and hence are not capable of correcting any errors. This follows from Theorems 4.2 and 4.3. So these codes can be of use only when Lee metric is under consideration.

The BCH code with d consecutive spectral components zeros has Hamming distance d+1 and hence corrects [(d+1)/2] errors, where [x] denotes the greatest integer less than or equal to x [12]. For these codes a decoding algorithm is obtained in Chapter 7 of this thesis, which is the counterpart of Berlekamp-Massey algorithm for BCH codes over finite fields.

For an arbitrary value of m, say $m=p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, a cyclic code C over Z_m is called a BCH code over Z_m if in the

decomposition of C as a direct sum of cyclic codes over $Z_{p_i^{k_i}}$, i=1,2,...s, as given in Theorem 4.3, each component code is a BCH code over $Z_{p_i^{k_i}}$, defined by the same set of d consecutive spectral components for all component codes.

Example 4.11: Let us consider the case m=6 and n=5. There are two conjugacy classes, {0} and {1,2,3,4}. We have

$$Z_6[x]/(x5-1) \equiv GR(2,1) \oplus GR(3,1) \oplus GR(2,4) \oplus GR(3,4).$$

By choosing full ring GR(2,1) ⊕ GR(3,1) for the conjugacy class {0} and the ideal GR(2,4) of the full ring GR(2,4) ⊕ GR(3,4) for the conjugacy class {1,2,3,4}, we obtain a generalised BCH code whose codewords are listed in Appendix D.

CHAPTER 5

ABELIAN CODES OVER Z_m

Over finite fields, Abelian codes have been studied by several authors [32-36]. Abelian codes over finite fields have better error correcting capabilities than cyclic codes over finite fields of the same length in some cases. For a given code length n, if a sufficiently great number of primes occur in the expansion of n, then the Abelian codes of length n have better error correcting capabilities compared to the cyclic codes of length n [33,34]. Among Abelian codes some of them, called separable codes, are Kronecker products of cyclic codes and others, called non-separable codes, cannot be obtained as Kronecker products of cyclic codes. Some good non-separable Abelian codes have been constructed by Camion [32]. The transform domain characterisation of Abelian codes over finite fields with mixed-radix number system as indexing scheme for DFT coefficients is discussed in [37]. Abelian codes over Z_m have been discussed in [13], by Wasan. In this chapter Abelian codes over Z_m are discussed in the transform domain.

Abelian codes over Z_m are a generalisation of cyclic codes over Z_m. The main difference between cyclic codes and Abelian codes is in defining the conjugacy class, which arises due to the change in indexing scheme. In the case of cyclic codes, the index

set (0,1,...,n-1) used for DFT coefficients as well as codeword components has the structure of a cyclic group which is commensurate with the structure of cyclic codes. In the case of Abelian codes, the DFT coefficients and codeword components are indexed in accordance with appropriate mixed-radix number system which is commensurate with the structure of abelian group. This leads to a different notion of conjugacy class.

For a given code length n, some of the Abelian codes of length n over Z_{p^k} may actually be cyclic codes of length n over Z_{p^k}. These codes which are Abelian and cyclic has the advantage of permitting one to work in a smaller extension ring compared to the extension ring required if only considered as a cyclic code. For the case of Abelian codes over finite fields, this aspect has been discussed in detail in [26]. In particular the following topics have been discussed in [26] (i) for what values of n and for which abelian groups all Abelian codes are cyclic (ii) given an abelian group of order n, identifying the cyclic codes among the Abelian codes and the number of them. These results have been obtained using Chinese Remainder Theorem (CRT) mapping [38] and mixed-radix mapping [26] along with the notion of conjugacy classes in mixed-radix number systems. Both CRT mapping and mixed-radix mapping are same when one considers codes over finite fields or Z_{p^k}. In this chapter (Subsection 5.3.1) we prove that the structure of conjugacy classes are also same for Abelian codes over GF(p) and Z_{p^k}. Hence results obtained in [26] hold

true for Abelian codes over Z_{p^k} also, with the only difference that instead of zeros in spectral components for the finite field case, nontrivial ideals also, apart from zeros, can be present in the case of Z_{p^k}.

In this chapter we obtain transform domain characterisation of Abelian codes over Z_m, by defining Generalised DFT using mixed-radix number system for indexing transform coefficients. Mixed-radix number systems are reviewed briefly in Section 5.1, and Abelian codes over Z_m are defined in Section 5.2. DFT over an Abelian group suitable for Abelian codes over Z_m is defined in Section 5.3, and conjugacy class structure in the setting of mixed-radix number system is discussed. Transform domain characterisation of Abelian codes over Z_{p^k} is obtained in Section 5.4. The cases, m being an arbitrary integer and a product of distinct primes respectively are considered in Section 5.5 and Section 5.6.

5.1 MIXED-RADIX NUMBER SYSTEM [39,40]

A number system is called a weighted number system if any number α can be uniquely expressed in the form

$$\alpha = \sum_i \alpha_i w_i$$

for some set of integers α_i's called digits and w_i's called weights. If the weights are successive powers of the same number

the number system is called fixed-radix number system otherwise a mixed-radix number system. Any number β in a mixed-radix number system can be expressed in the form

$$\beta = \sum_i \beta_i \left(\prod_{j=0}^{i-1} m_j \right)$$

The m_i's are called the mixed radices and β_i's are called mixed-radix digits, where $0 \leq \beta_i < m_i$.

Let $m_0, m_1, \ldots, m_{r-1}$ be a set of positive integers. Then with respect to the above numbers as mixed radices, any nonnegative integer α, where $0 \leq \alpha \leq \left(\prod_{k=0}^{r-1} m_k - 1 \right)$ can be uniquely expressed as

$$\alpha = \alpha_{r-1}\left(\prod_{j=0}^{r-2} m_j \right) + \alpha_{r-2}\left(\prod_{j=0}^{r-3} m_j \right) + \ldots + \alpha_2(m_0 m_1) + \alpha_1(m_0) + \alpha_0$$

The weight of α_0 is unity. The mixed-radix representation of an integer α is denoted by $< \alpha_{r-1}, \alpha_{r-2}, \ldots, \alpha_1, \alpha_0 >$ or simply by $< \alpha >$, where the mixed radices are understood.

Let $\langle i \rangle = \langle i_{r-1}, i_{r-2}, \ldots, i_0 \rangle$ and $\langle j \rangle = \langle j_{r-1}, j_{r-2}, \ldots, j_0 \rangle$ be the mixed-radix representations of the integer i, j with radices $m_0, m_1, \ldots, m_{r-1}$. The operations of addition and subtraction denoted respectively by $\dot{+}$ and $\dot{-}$ are defined by

$$i \dot{+} j = \langle i \rangle \dot{+} \langle j \rangle = \langle (i_{r-1}+j_{r-1})_{m_{r-1}}, \ldots, (i_0+j_0)_{m_0} \rangle$$

$$i \dot{-} j = \langle i \rangle \dot{-} \langle j \rangle = \langle (i_{r-1}-j_{r-1})_{m_{r-1}}, \ldots, (i_0-j_0)_{m_0} \rangle$$

where $(i_q+j_q)_{m_q}$ and $(i_q-j_q)_{m_q}$ denote addition and subtraction modulo m_q.

Example 5.1

Let the mixed radices be $m_0=3$ and $m_1=5$. The weights of the digits are 1 for i_0 and 3 for i_1. The conversion of numbers 0 to 14 in this mixed radix number system is shown in Table 5.1.

Example 5.2

Let the mixed radices be $m_0=3$ and $m_1=3$. The weight for i_0 is 1 and the weight for i_1 is 3. The numbers 0 to 8 are expressed in this mixed-radix system as shown in Table 5.2.

Mixed radix number system can be used as an indexing scheme for the elements of a finite Abelian group in accordance with the notion of representing numbers with respect to mixed radices, the mixed radices being the orders of the cyclic subgroups the direct products of which give the Abelian group, which results in a simpler way of specifying the group operation.

It is easy to see that an Abelian group G of order n, which is the direct product of cyclic subgroups of orders $m_0, m_1, \ldots, m_{r-1}$ is completely specified by the rule of composition for the group elements

$$g_i g_j = g_{i \dot{+} j} \qquad i, j \in (0,1,\ldots,n-1)$$

where $\dot{+}$ denotes addition in the mixed-radix number system with radices $m_0, m_1, \ldots, m_{r-1}$. It is understood that the i-th element of G, g_i, $i \in (0,1,\ldots,n-1)$, is represented by

Table 5.1 Mixed-radix numbers corresponding to Example 5.1.

Number	Mixed-radix digits	
	i_1	i_0
0	0	0
1	0	1
2	0	2
3	1	0
4	1	1
5	1	2
6	2	0
7	2	1
8	2	2
9	3	0
10	3	1
11	3	2
12	4	0
13	4	1
14	4	2

The number corresponding to <3,2> is 3(3)+2(1)=11.

Table 5.2 Mixed-radix numbers corresponding to Example 5.2.

Number	Mixed-radix digits	
	i_1	i_0
0	0	0
1	0	1
2	0	2
3	1	0
4	1	1
5	1	2
6	2	0
7	2	1
8	2	2

$$g_i = g_{\langle i_{r-1}, i_{r-2}, \ldots, i_0 \rangle}$$

when $$g_i = (\alpha_{m_{r-1}})^{i_{r-1}} (\alpha_{m_{r-2}})^{i_{r-2}} \ldots (\alpha_{m_0})^{i_0}$$

where $\alpha_{m_{r-1}}, \alpha_{m_{r-2}}, \ldots, \alpha_{m_0}$ are generators of cyclic subgroups of orders respectively $m_{r-1}, m_{r-2}, \ldots, m_0$.

5.2 ABELIAN CODES OVER Z_m

Let G denote an abelian group of order n which is a direct product of v cyclic subgroups of orders $n_0, n_1, \ldots, n_{v-1}$. The group ring GZ_m is the set of formal sums given by

$$GZ_m = \left(\sum_{g \in G} c_g g : c_g \in Z_m \right)$$

If $\alpha_{n_0}, \alpha_{n_1}, \ldots, \alpha_{n_{v-1}}$ are the generators of cyclic subgroups then any element $g \in G$ can be written as

$$g = (\alpha_{n_0})^{i_0} (\alpha_{n_1})^{i_1} \ldots (\alpha_{n_{v-1}})^{i_{v-1}}$$

for some $i_0, i_1, \ldots i_{v-1}$, where $0 \leq i_k \leq n_k - 1$, $k = 0, 1, \ldots, v-1$. This element g is denoted by g_i. Then

$$GZ_m = \left(\sum_{i=0}^{n-1} c_i g_i : c_i \in Z_m \right)$$

or equivalently any element c in GZ_m is of the form

$$c = \sum_{i_{v-1}=0}^{n_{v-1}-1} \sum_{i_{v-2}=0}^{n_{v-2}-1} \cdots \sum_{i_0=0}^{n_0-1} c_{\langle i_0, i_1 \ldots i_{v-1} \rangle} g_{\langle i_0, i_1, \ldots i_{v-1} \rangle}$$

$$= \sum_{\langle i \rangle = 0}^{n-1} c_{\langle i \rangle} g_{\langle i \rangle} .$$

There is a natural one-to-one correspondence between the set of n-tuples over Z_m, denoted by Z_m^n, and GZ_m given by

$$(c_0, c_1, \ldots, c_{n-1}) \longleftrightarrow (c_{\langle 0\rangle}, c_{\langle 1\rangle}, \ldots, c_{\langle n-1\rangle}).$$

Addition and multiplication in GZ_m are given by

$$\sum_{\langle i\rangle=0}^{n-1} c_{\langle i\rangle} a_{\langle i\rangle} + \sum_{\langle i\rangle=0}^{n-1} d_{\langle i\rangle} a_{\langle i\rangle} = \sum_{\langle i\rangle=0}^{n-1} (c_{\langle k\rangle} + d_{\langle k\rangle}) a_{\langle k\rangle}$$

and

$$\sum_{\langle i\rangle=0}^{n-1} c_{\langle i\rangle} a_{\langle i\rangle} \sum_{\langle i\rangle=0}^{n-1} d_{\langle j\rangle} a_{\langle j\rangle} = \sum_{\langle k\rangle=0}^{n-1} e_{\langle k\rangle} a_{\langle k\rangle}$$

where

$$e_{\langle k\rangle} = \sum_{\langle i\rangle=0}^{n-1} c_{\langle i\rangle} d_{(\langle k\rangle - \langle i\rangle)} .$$

Definition 5.1: Given an Abelian group G of order n, an Abelian code of length n over Z_m is the set of n-tuples over Z_m, which correspond to an ideal of the Group ring GZ_m.

A cyclic code over Z_m is a submodule of Z_m^n with the property that it is closed under cyclic convolution. The multiplication operation of group ring is a generalisation of cyclic convolution and an abelian code over Z_m is a submodule of Z_m^n which is closed under this generalised convolution. In the next section we develop a transform over an extension ring of Z_{p^k} which isomorphically maps this generalised convolution to pointwise multiplication. This transform will be referred as Generalised Discrete Fourier Transform (GDFT).

5.3 GENERALISED DFT

Throughout this section it is assumed that $m = p^k$.

Let G be an Abelian group of order n which is a direct product of v cyclic sugbroups of orders $n_0, n_1, \ldots, n_{v-1}$ respectively. Let n' be the exponent of G. (We recall that the exponent of an Abelian group is the maximum of the orders of its elements.) Choose the least integer r such that n' divides (p^r-1). In $GR^*(p^k,r)$ there exists elements $\alpha_{n_0}, \alpha_{n_1}, \ldots, \alpha_{n_{v-1}}$ of order $n_0, n_1, \ldots n_{v-1}$ respectively.

Definition 5.2: Let $a = (a_{<0>}, a_{<1>}, \ldots, a_{<n-1>}) \in Z_{p^k}^n$. The transform vector $A = (A_{<0>}, A_{<1>}, \ldots, A_{<n-1>})$ of a is given by

$$A_{<j>} = \sum_{i_{v-1}=0}^{n_{v-1}-1} \cdots \sum_{i_0=0}^{n_0-1} (\alpha_{n_0})^{i_0 j_0} \ldots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}} a_{<i_0, \ldots i_{v-1}>}$$

where $<j> = <j_0, j_1, \ldots, j_{v-1}>$ and $<i> = <i_0, i_1, \ldots, i_{v-1}>$ are the mixed-radix number representations with indices $n_0, n_1, \ldots, n_{v-1}$.

The set of all n-tuples over $GR(p^k,r)$ which are transform vectors of some n-tuple over Z_{p^k} is denoted by $F(GZ_{p^k})$. Our purpose is to show that this transform defines an isomorphism and then to identify the subalgebra $F(GZ_{p^k})$ of the pointwise product algebra of n-tuples over $GR(p^k,r)$. Towards this end a theorem from [22] is given below without proof.

Theorem 5.1: [22,Theorem 2] Let R be a local ring and G a finite Abelian group of order n and exponent m. Then R supports a discrete Fourier transform over G if and only if

(a) R contains a primitive m-th root of unity.

(b) m is a unit in R.

In the proof of the above theorem the DFT has been shown to be an isomorphism given by

$$U\Big(\sum_{g\in G} r_g g\Big) = \sum_{g\in G}\Big(\sum_{j=0}^{n-1} u_j(g)\Big) r_g$$

where $r_g \in R$ and u_j, $j=0,1,\ldots,n-1$, constitute a group of homomorphisms of G into the group of units of R.

It can be checked that the set of mappings u_j: G ---> $GR^*(p^k,r)$, $j=0,1,\ldots,n-1$, given by

$$u_j(g^{<i>}) = (\alpha_{n_0})^{i_0 j_0} (\alpha_{n_1})^{i_1 j_1} \ldots\ldots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}}$$

constitute the set of all homomorphisms of G into $GR^*(p^k,r)$. From Theorem 5.1 it follows that the DFT defined in Definition 5.2 establishes an isomorphism between the convolution algebra GZ_{p^k} and a subalgebra of $GR^n(p^k,r)$, which is $F(GZ_{p^k})$. To identify this $F(GZ_{p^k})$ we first modify the notion of conjugacy class in the setting of mixed-radix number system in the next section.

5.3.1 Conjugacy classes for mixed-radix number systems

Our aim is to identify which DFT coefficients of a transform vector $(A_{<0>},A_{<1>},\ldots,A_{<n-1>})$ are related.

Theorem 5.2: [24,Theorem XV] In $GR(p^k,r)$ there exists a primitive element α such that the cyclic group of automorphisms of $GR(p^k,r)$ which keeps Z_{p^k} invariant has the generator σ given by $\sigma(\alpha) = \alpha^p$.

Using the above theorem we obtain the conjugacy constraint for Abelian codes in the following theorem.

Theorem 5.3 If $(A_{<0>},A_{<1>},\ldots,A_{<n-1>}) \in GR^n(p^k,r)$ is GDFT of $(a_{<0>},a_{<1>},\ldots,a_{<n-1>})$ then the following relation among $A_{<i>}$, $i=0,1,\ldots,n-1$ holds.

$$\sigma(A_{<j>}) = A_{p<j>}$$

where σ is a generator of the automorphism group of $GR(p^k,r)$ and $p_{<j>}$ stands for $<pj_0 \pmod{n_0}, pj_1 \pmod{n_1}, \ldots, pj_{v-1} \pmod{n_{v-1}}>$.

Proof: From Theorem 5.2, it follows that there exists a primitive element α in $GR(p^k,r)$ such that $\sigma(\alpha) = \alpha^p$.

Let $$\alpha = (\alpha_{n_0})^{t_0} (\alpha_{n_1})^{t_1} \ldots (\alpha_{n_{v-1}})^{t_{v-1}} \qquad (5.1)$$

for some integers $t_0,t_1,\ldots,t_{v-1}$, where α_{n_i} is an element of $GR^*(p^k,r)$ of order n_i, where n_i, $i=0,1,\ldots v-1$, are the mixed radices. Then $\sigma(\alpha) = \alpha^p$ implies

$$\sigma(\alpha) = (\alpha_{n_0})^{pt_0} (\alpha_{n_1})^{pt_1} \ldots\ldots (\alpha_{n_{v-1}})^{pt_{v-1}} .$$

Since

$$A_{<j>} = \sum_{<i>=0}^{n-1} (\alpha_{n_0})^{i_0 j_0} (\alpha_{n_1})^{i_1 j_1} \ldots\ldots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}} \; a_{<i>} ,$$

we have

$$\sigma(A_{<j>}) = \sum_{<i>=0}^{n-1} a_{<i>} \; \sigma((\alpha_{n_0})^{i_0 j_0} (\alpha_{n_1})^{i_1 j_1} \ldots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}})$$

$$= \sum_{<i>=0}^{n-1} a_{<i>} \; (\sigma(\alpha_{n_0}))^{i_0 j_0} (\sigma(\alpha_{n_1}))^{i_1 j_1} \ldots (\sigma(\alpha_{n_{v-1}}))^{i_{v-1} j_{v-1}}$$

$$= \sum_{<i>=0}^{n-1} a_{<i>} \; (\alpha_{n_0})^{p i_0 j_0} (\alpha_{n_1})^{p i_1 j_1} \ldots (\alpha_{n_{v-1}})^{p i_{v-1} j_{v-1}}$$

if we assume $\sigma(\alpha_{n_i}) = \alpha_{n_i}^{p}$ for $i=0,1,\ldots,v-1$.

$$= A_{p<j>}$$

where $p_{<j>}$ denotes $<pj_0 (\mathrm{mod}\ n_0), pj_1 (\mathrm{mod}\ n_1), \ldots, pj_{v-1} (\mathrm{mod}\ n_{v-1})>$. Hence what remains to prove is that one can always choose α_{n_i}, $i=0,1,\ldots,v-1$, in (5.1) such that $\sigma^{-1}(\alpha_{n_i}^{p}) = \alpha_{n_i}$.

Let G_1 denote the cyclic subgroup of order (p^r-1) in $GR^*(p^k,r)$. Since σ is an automorphism, elements of G_1 are mapped onto elements of G_1 and elements of particular order are mapped onto elements of the same order. For a chosen α_{n_i}, $i=0,1,\ldots,s-1$, if $\sigma(\alpha_{n_i}) \neq \alpha_{n_i}^{p}$, let $\sigma(\alpha_{n_i}) = (\alpha_{n_i})^{c_i}$ for some integer c_i. Let G_i denote the subgroup generated by α_{n_i}. The generators of G_i are $(\alpha_{n_i})^{\beta_1}, (\alpha_{n_i})^{\beta_2}, \ldots, (\alpha_{n_i})^{\beta_t}$, where t is equal to $\phi(n_i)$, Euler's

totient function, and $\beta = (\beta_1, \beta_2, \ldots, \beta_t)$ set of all integers less than n_i and relatively prime to n_i. The set of elements $c_i\beta_1, c_i\beta_2, \ldots, c_i\beta_t$ each modulo n_i, also form β. Moreover, since p and n_i are realtively prime, $p \in \beta$. Hence for some j, $j=1,2,\ldots,t$, we have $c_i\beta_j = p \pmod{n_i}$. Then our choice is $(\alpha_{n_i})^{\beta_j}$ for α_{n_i}. For this choice the relation $\sigma(\alpha_{n_i}) = \alpha_{n_i}^{p}$ holds. Q.E.D.

From Theorem 5.3 it is easy to see that the conjugacy class containing $\langle j \rangle$ is $\{\langle j \rangle, p\langle j \rangle, \ldots, p^{e-1}\langle j \rangle\}$ where e is the exponent, i.e., $p^e\langle j \rangle = \langle j \rangle$.

Definition 5.3: Let $n = n_0\, n_1 \ldots n_{v-1}$ and p be a prime relatively prime to n. For the mixed-radix number system with mixed radices $n_0, n_1, \ldots, n_{v-1}$, the conjugacy class containing $\langle j \rangle$, denoted by $C_{p,n}(\langle j \rangle)$, $0 \leq j \leq n-1$, is the set $\{\langle j \rangle, p\langle j \rangle, p^2\langle j \rangle, \ldots, p^{e-1}\langle j \rangle\}$ where $p^e\langle j \rangle = \langle j \rangle$ and e is called the exponent of the conjugacy class.

It is proved in [37] that for the case of Abelian codes of length n over GF(p) the conjugacy classes are same as given above.

Example 5.3: For different values of n with mixed radices n_0, n_1, and for a prime p, relatively prime to n, all the conjugacy classes are listed in Table 5.3.

Table 5.3 Listing of conjugacy classes in some mixed-radix number systems

p	n	n_0	n_1	conjugacy classes
2	9	3	3	{ <00> }, { <01>, <02> }, { <10>, <20> }, { <11>, <22> }, { <12>, <21> }.
2	15	3	5	{ <00> }, { <01>, <02>, <04>, <03> }, { <10>, <20> }, { <11>, <22>, <14>, <23> }, { <12>, <24>, <13>, <21> }.
2	25	5	5	{ <00> }, { <01>, <02>, <04>, <03> }, { <10>, <20>, <40>, <30> }, { <11>, <22>, <44>, <33> }, { <12>, <24>, <43>, <31> }, { <13>, <21>, <34>, <42> }, { <14>, <23>, <32>, <41> }.
2	21	3	7	{ <00> }, { <01>, <02>, <04> }, { <03>, <06>, <05> }, { <10>, <20> }, { <11>, <22>, <14>, <21>, <12>, <24> }, { <13>, <26>, <15>, <23>, <16>, <25> }.
3	8	2	4	{ <00> }, { <01>, <03> }, { <02> }, { <10> }, { <11>,<13> }, { <12> }.
3	10	2	5	{ <00> }, { <01>, <03>, <04>, <02> }, { <10> }, { <11>, <13>, <14>, <12> }.

(Table 5.3 continued)

```
3  14   2   7   { <00> }, { <10> },
                 { <01>, <03>, <02>, <06>, <04>, <05> },
                 { <11>, <13>, <12>, <16>, <14>, <15> }.

3  20   4   7   { <00> },  { <20> },  { <10>, <30> },
                 { <01>, <03>, <04>, <02> },
                 { <11>, <33>, <14>, <32> },
                 { <12>, <31>, <13>, <34> },
                 { <21>, <23>, <24>, <22> }.
```

The following theorem proved in [26] gives the number of conjugacy classes for given n and p.

Theorem 5.4: [26] Let $n = n_0\, n_1 \ldots n_{v-1}$ and p be a prime relatively prime to n. The number of conjugacy classes, denoted by N, in the mixed-radix number system with mixed radices $n_0, n_1, \ldots, n_{v-1}$ is given by

$$N = \sum_{d_0 | n_0} \sum_{d_1 | n_1} \cdots \sum_{d_{v-1} | n_{v-1}} \frac{\emptyset(d_0)\, \emptyset(d_1) \cdots \emptyset(d_{v-1})}{\text{l.c.m.}\,(e_0, e_1, \ldots, e_{v-1})}$$

where $e_i = \exp_p(d_i)$, $i = 0, 1, \ldots, v-1$.

We have identified which GDFT coefficients are related and the actual relation is determined by the generator of the automorphism group of $GR(p^k, r)$. i.e., if $A_{<j>}$ is $a_0 + a_1 x + a_2 x^2 + \ldots + a_{r-1} x^{r-1}$, then $A_{p<j>}$ is given by $a_0 + a_1 \sigma(x) + a_2 (\sigma(x))^2 + \ldots + a_{r-1} (\sigma(x))^{r-1}$, where $\sigma(x) \in GR(p^k, r)$ is the image of $x \in GR(p^k, r)$ under the automorphism σ.

5.4 SPECTRAL CHARACTERISATION OF ABELIAN CODES OVER Z_{p^k}

In the case of cyclic codes over Z_{p^k} it was seen that the set consisting of images under DFT of all n-tuples over Z_{p^k} is isomorphic to a direct sum of certain subrings of the extension ring (Galois ring). In this section it is shown that for Abelian codes also this is true. i.e., the set of all images under GDFT

of all n-tuples over Z_{p^k}, denoted by $F[GZ_{p^k}]$, is isomorphic to a direct sum of Galois rings, which are subrings of the extension ring. This isomorphism leads to the spectral characterisation of Abelian codes over Z_{p^k}.

Theorem 5.5: $$F[GZ_{p^k}] \equiv \bigoplus_{i=1}^{t} GR(p^k, r_i)$$

where t is the number of conjugacy classes in the mixed-radix system corresponding to the factorisation of G into direct product of its cyclic subgroups and r_i, i=1,2,...,t, exponents of the conjugacy classes.

Proof: For a fixed $\langle j \rangle$, $0 \leq j \leq n-1$, let the conjugacy class $C_{p,n}(\langle j \rangle)$ have exponent e. Let $(A_{\langle 0 \rangle}, A_{\langle 1 \rangle}, \ldots, A_{\langle n-1 \rangle})$ be any transform vector. Because of the conjugacy symmetry property it is required that $\sigma(A_{p^{e-1}j}) = A_{\langle p^e j \rangle}$, i.e., $\sigma^e(A_{\langle k \rangle}) = A_{\langle k \rangle}$ for all $\langle k \rangle$ in the conjugacy class $C_{p,n}(\langle j \rangle)$, where σ is a generator of the automorphism group of $GR(p^k, r)$. In other words $A_{\langle k \rangle}$ is an element of degree e in $GR(p^k, r)$ and hence belong to the subring $GR(p^k, e)$. Let R_j denote the subset of $F[GZ_{p^k}]$ consisting of only those elements of $F[GZ_{p^k}]$ which have all spectral components zero except the ones that belong to $C_{p,n}(\langle j \rangle)$. Since the value of one DFT component of a conjugacy class uniquely specify the other values in the conjugacy class, we have

$$R_j \equiv GR(p^k, e).$$

Since the conjugacy classes are disjoint and the operations are

pointwise it follows that

$$F[GZ_{p^k}] \equiv R_{j_1} \circledast R_{j_2} \circledast \ldots \circledast R_{j_t}$$

where $j_1, j_2, \ldots, j_t$ belong to different conjugacy classes and t is the number of conjugacy classes. From the above isomorphism we have

$$F[GZ_{p^k}] \equiv \mathop{\circledast}_{i=0}^{t} GR(p^k, r_i)$$

where r_i is the exponent of the i-th conjugacy class. Q.E.D.

It may be noted that the expression for $F[GZ_{p^k}]$ is identical to the expression obtained for R_T in the case of cyclic codes, except that t denotes the number of conjugacy classes in different number systems, (in a mixed-radix number system for Abelian codes and in a fixed-radix number system for cyclic codes) resulting in r_i, i=1,2,...,t, representing exponents of the conjugacy classes in corresponding number systems.

From Theorem 5.5 the following spectral characterisation of Abelian codes follows.

Definition 5.4: Let G be an Abelian group of order n which is direct product of v cyclic subgroups of order $n_0, n_1, \ldots, n_{v-1}$. Also let t be the number of conjugacy classes, in the mixed-radix number system with radices $n_0, n_1, \ldots, n_{v-1}$, with exponents r_i, i=1,2,...,t. Then Abelian codes of length n over Z_{p^k} are the

inverse GDFT of n-tuples over $Z_p k$ corresponding to the ideals of the ring $\bigoplus_{i=0}^{t} GR(p^k, r_i)$.

From Definition 5.4, it follows that any Abelian code is of the form

$$L \equiv \bigoplus_{i=1}^{t} p^{j_i} GR(p^k, r_i) \qquad 0 \leq j_i \leq k$$

and we define minimal and subminimal Abelian codes, as in the case of cyclic codes, as follows.

Abelian codes which are of the form

$$L_{<i>} \equiv GR(p^k, r_i) \qquad i=1,2,\ldots,t$$

are called minimal Abelian codes and the Abelian codes of the form

$$L_{<i>,j_i} \equiv p^{j_i} GR(p^k, r_i) \; ; \qquad 0 < j_i < k$$

are called subminimal Abelian codes corresponding to L_i.

The wordlength μ of L is given by

$$\mu = \sum_{i=1}^{t} r_i (k - j_i)$$

and the number of nontrivial cyclic codes for given n and p^k is $((k+1)^t - 2)$.

It can be checked that Theorem 4.2 and Theorem 4.3, regarding minimum Hamming distance of cyclic codes are valid for Abelian codes also.

It is observed that given n and p^k, the expressions for cyclic and Abelian codes are same and also the number of nontrivial codes, wordlength and the number of codewords in each Abelian code have the same expression as in the case of cyclic codes. The difference appears in the number of conjugacy classes and exponents of the conjugacy classes.

Example 5.4: Let us consider the noncyclic group of order 9 and Z_4. There are 5 conjugacy classes and the appropriate extension ring is GR(4,2). There are 3 ideals in GR(4,2) including trivial ones. Hence there are $3^5-2 = 241$ Abelian codes. We have

$$GZ_4[x] \equiv GR(4,1) \oplus GR(4,2) \oplus GR(4,2) \oplus GR(4,2) \oplus GR(4,2)$$

where G denotes the abelian group. There are five conjugacy classes {<00>}, {<01>,<02>}, {<10>,<20>}, {<11>,<22>}, and {<12>,<21>}. So there are five minimal codes and corresponding to each minimal code there is one subminimal code.

We have listed in Table 5.4, codewords of all minimal and subminimal Abelian codes.

Table 5.4 Complete listing of minimal and subminimal Abelian codes of length 9 over Z_4.

code 1: Minimal code $L_{\langle 00\rangle}$.

$C_{2,9}(\langle 00\rangle)$ takes value from the ideal GR(4,1) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
1	1	1	1	1	1	1	1	1	10	00	00	00	00	00	00	00	00
2	2	2	2	2	2	2	2	2	20	00	00	00	00	00	00	00	00
3	3	3	3	3	3	3	3	3	30	00	00	00	00	00	00	00	00

code 2: Subminimal code $L_{\langle 00\rangle,1}$.

$C_{2,9}(\langle 00\rangle)$ takes value from the ideal 2GR(4,1) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
2	2	2	2	2	2	2	2	2	20	00	00	00	00	00	00	00	00

(Table 5.4 continued)

code 3: Minimal code $L_{\langle 01\rangle}$.

$C_{2,9}(\langle 01\rangle)$ takes value from the ideal GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	1	3	0	1	3	0	1	3	00	12	32	00	00	00	00	00	00
0	2	2	0	2	2	0	2	2	00	20	20	00	00	00	00	00	00
0	3	1	0	3	1	0	3	1	00	32	12	00	00	00	00	00	00
1	0	3	1	0	3	1	0	3	00	31	23	00	00	00	00	00	00
1	1	2	1	1	2	1	1	2	00	03	11	00	00	00	00	00	00
1	2	1	1	2	1	1	2	1	00	11	03	00	00	00	00	00	00
1	3	0	1	3	0	1	3	0	00	23	31	00	00	00	00	00	00
2	0	2	2	0	2	2	0	2	00	22	02	00	00	00	00	00	00
2	1	1	2	1	1	2	1	1	00	30	30	00	00	00	00	00	00
2	2	0	2	2	0	2	2	0	00	02	22	00	00	00	00	00	00
2	3	3	2	3	3	2	3	3	00	10	10	00	00	00	00	00	00
3	0	1	3	0	1	3	0	1	00	13	21	00	00	00	00	00	00
3	1	0	3	1	0	3	1	0	00	21	13	00	00	00	00	00	00
3	2	3	3	2	3	3	2	3	00	33	01	00	00	00	00	00	00
3	3	2	3	3	2	3	3	2	00	01	33	00	00	00	00	00	00

code 4: Subminimal code $L_{\langle 01\rangle,1}$.

$C_{2,9}(\langle 01\rangle)$ takes value from the ideal 2GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	2	2	0	2	2	0	2	2	00	20	20	00	00	00	00	00	00
2	0	2	2	0	2	2	0	2	00	22	02	00	00	00	00	00	00
2	2	0	2	2	0	2	2	0	00	02	22	00	00	00	00	00	00

(Table 5.4 continued)

code 5: Minimal code $L_{\langle 1,0\rangle}$.

$C_{2,9}(\langle 10\rangle)$ takes value from the ideal GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	0	0	1	1	1	3	3	3	00	00	00	12	00	00	32	00	00
0	0	0	2	2	2	2	2	2	00	00	00	20	00	00	20	00	00
0	0	0	3	3	3	1	1	1	00	00	00	32	00	00	12	00	00
1	1	1	0	0	0	3	3	3	00	00	00	31	00	00	23	00	00
1	1	1	1	1	1	2	2	2	00	00	00	03	00	00	11	00	00
1	1	1	2	2	2	1	1	1	00	00	00	11	00	00	03	00	00
1	1	1	3	3	3	0	0	0	00	00	00	23	00	00	31	00	00
2	2	2	0	0	0	2	2	2	00	00	00	22	00	00	02	00	00
2	2	2	1	1	1	1	1	1	00	00	00	30	00	00	30	00	00
2	2	2	2	2	2	0	0	0	00	00	00	02	00	00	22	00	00
2	2	2	3	3	3	3	3	3	00	00	00	10	00	00	10	00	00
3	3	3	0	0	0	1	1	1	00	00	00	13	00	00	21	00	00
3	3	3	1	1	1	0	0	0	00	00	00	21	00	00	13	00	00
3	3	3	2	2	2	3	3	3	00	00	00	33	00	00	01	00	00
3	3	3	3	3	3	2	2	2	00	00	00	01	00	00	33	00	00

code 6: Subminimal code $L_{\langle 1,0\rangle,1}$.

$C_{2,9}(\langle 10\rangle)$ takes value from the ideal 2GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	0	0	2	2	2	2	2	2	00	00	00	20	00	00	20	00	00
2	2	2	0	0	0	2	2	2	00	00	00	22	00	00	02	00	00
2	2	2	2	2	2	0	0	0	00	00	00	02	00	00	22	00	00

(Table 5.4 continued)

code 7: Minimal code $L_{\langle 11\rangle}$.

$C_{2,9}(\langle 11\rangle)$ takes value from the ideal GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	1	3	1	3	0	3	0	1	00	00	00	00	12	00	00	00	32
0	2	2	2	2	0	2	0	2	00	00	00	00	20	00	00	00	20
0	3	1	3	1	0	1	0	3	00	00	00	00	32	00	00	00	12
1	0	3	0	3	1	3	1	0	00	00	00	00	31	00	00	00	23
1	1	2	1	2	1	2	1	1	00	00	00	00	03	00	00	00	11
1	2	1	2	1	1	1	1	2	00	00	00	00	11	00	00	00	03
1	3	0	3	0	1	0	1	3	00	00	00	00	23	00	00	00	31
2	0	2	0	2	2	2	2	0	00	00	00	00	22	00	00	00	02
2	1	1	1	1	2	1	2	1	00	00	00	00	30	00	00	00	30
2	2	0	2	0	2	0	2	2	00	00	00	00	02	00	00	00	22
2	3	3	3	3	2	3	2	3	00	00	00	00	10	00	00	00	10
3	0	1	0	1	3	1	3	0	00	00	00	00	13	00	00	00	21
3	1	0	1	0	3	0	3	1	00	00	00	00	21	00	00	00	13
3	2	3	2	3	3	3	3	2	00	00	00	00	33	00	00	00	01
3	3	2	3	2	3	2	3	3	00	00	00	00	01	00	00	00	33

code 8: Subminimal code $L_{\langle 11\rangle,1}$.

$C_{2,9}(\langle 11\rangle)$ takes value from the ideal 2GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	2	2	2	2	0	2	0	2	00	00	00	00	20	00	00	00	20
2	0	2	0	2	2	2	2	0	00	00	00	00	22	00	00	00	02
2	2	0	2	0	2	0	2	2	00	00	00	00	02	00	00	00	22

(Table 5.4 continued)

code 9: Minimal code $L_{\langle 12\rangle}$.

$C_{2,9}(\langle 12\rangle)$ take value from the ideal GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	1	3	3	0	1	1	3	0	00	00	00	00	00	32	00	12	00
0	2	2	2	0	2	2	2	0	00	00	00	00	00	20	00	20	00
0	3	1	1	0	3	3	1	0	00	00	00	00	00	12	00	32	00
1	0	3	3	1	0	0	3	1	00	00	00	00	00	23	00	31	00
1	1	2	2	1	1	1	2	1	00	00	00	00	00	11	00	03	00
1	2	1	1	1	2	2	1	1	00	00	00	00	00	03	00	11	00
1	3	0	0	1	3	3	0	1	00	00	00	00	00	31	00	23	00
2	0	2	2	2	0	0	2	2	00	00	00	00	00	02	00	22	00
2	1	1	1	2	1	1	1	2	00	00	00	00	00	30	00	30	00
2	2	0	0	2	2	2	0	2	00	00	00	00	00	22	00	02	00
2	3	3	3	2	3	3	3	2	00	00	00	00	00	10	00	10	00
3	0	1	1	3	0	0	1	3	00	00	00	00	00	21	00	13	00
3	1	0	0	3	1	1	0	3	00	00	00	00	00	13	00	21	00
3	2	3	3	3	2	2	3	3	00	00	00	00	00	01	00	33	00
3	3	2	2	3	3	3	2	3	00	00	00	00	00	33	00	01	00

code 10: Subminimal code $L_{\langle 12\rangle,1}$.

$C_{2,9}(\langle 12\rangle)$ takes value from the ideal 2GR(4,2) and other conjugacy classes take zero.

Codeword									Spectrum								
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7	A_8
0	0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00	00
0	2	2	2	0	2	2	2	0	00	00	00	00	00	20	00	20	00
2	0	2	2	2	0	0	2	2	00	00	00	00	00	02	00	22	00
2	2	0	0	2	2	2	0	2	00	00	00	00	00	22	00	02	00

5.5 ABELIAN CODES FOR $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$

In this section we obtain transform domain characterisation for Abelian codes for arbitrary value of m, $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$.

Let the Abelian group G under consideration be of order n and exponent n'. Let this be the direct product of v cyclic subgroups each of order $n_0, n_1, \ldots, n_{v-1}$. The extension ring of Z_m in which GDFT is defined is same as $Q(m,r) = Z_m[x]/\emptyset(x)$ obtained for the case of cyclic codes over Z_m in Subsection 4.2.1, with the only difference being that r is chosen such that the exponent n' divides g.c.d $((p_1^r-1),(p_2^r-1),\ldots,(p_s^r-1))$ instead of the order n.

From Lemma 4.1, the order of $Q^*(m,r)$ is given by N, where

$$N = \prod_{i=1}^{s} p_i^{r(k_i-1)} (p_i^r-1)$$

Since, $n_0, n_1, \ldots, n_{v-1}$, each divides n' and n' divides g.c.d. of $((p_1^r-1),(p_2^r-1),\ldots,(p_s^r-1))$ one can find elements $\alpha_{n_0}, \alpha_{n_1}, \ldots \alpha_{n_{v-1}}$ of orders $n_0, n_1, \ldots n_{v-1}$ respectively in $Q^*(m,r)$.

As in the case of $m = p^k$ the mappings u_j: G ---> $Q^*(m,r)$, j=0,1,...,n-1 given by

$$u_j(g^{<i>}) = (\alpha_{n_0})^{i_0 j_0} (\alpha_{n_1})^{i_1 j_1} \ldots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}}$$

constitute the set of all homomorphisms of G into Q(m,r) and

hence the GDFT for the case $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ is given by

Definition 5.5: Let $a = (a_{<0>}, a_{<1>}, \ldots, a_{<n-1>}) \in Z_m^n$. Then the transform vector of a, $A = (A_{<0>}, A_{<1>}, \ldots, A_{<n-1>}) \in Q^n(m,r)$ is given by

$$A_{<j>} = \sum_{i_{v-1}=0}^{n_{v-1}-1} \cdots \sum_{i_0=0}^{n_0-1} (\alpha_{n_0})^{i_0 j_0} \cdots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}} a_{<i_0, \ldots i_{v-1}>} \qquad j=0,1,\ldots,n-1$$

where $<j> = <j_0, j_1, \ldots j_{v-1}>$ and $<i> = <i_0, i_1, \ldots i_{v-1}>$ are mixed radix numbers with radices $n_0, n_1, \ldots, n_{v-1}$.

The group of automorphisms of $Q(m,r)$ has already been discussed in Subsection 4.2.1 and conjugacy classes for different p_i's and and n have been obtained in Subsection 5.3.1. The structure of the subring in $Q^n(m,r)$ which is the set of transform vectors of all n-tuples of Z_m denoted by $F[GZ_m]$ is given by

Theorem 5.6: The subring $F[GZ_m]$ of $Q^n(m,r)$ which contains all the transform vectors of n-tuples of Z_m, $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ is isomorphic to $\bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GR(p_i^{k_i}, e_{ij})$ where t_i is the number of conjugacy classes in the mixed-radix system and e_{ij}, $j=1,2,\ldots,t_i$, are the exponents corresponding to p_i.

Proof: The proof is similar to the proof of corresponding theorem for cyclic codes, Theorem 4.2 in Subsection 4.2.1. Q.E.D.

From Theorem 5.6 we obtain the following transform domain characterisation for Abelian codes over Z_m, $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$.

Definition 5.6: Let G be an Abelian group of order n which is direct product of v cyclic subgroups of order $n_0,n_1,\ldots,n_{v-1}$. Let t_i be the number of conjugacy classes in the mixed-radix number system with radices $n_0,n_1,\ldots,n_{v-1}$ corresponding to p_i, $i=1,2,\ldots,s$, with exponents e_{ij}, $j=1,2,\ldots,t_i$. An Abelian code of length n over Z_m, $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$ is the set of inverse GDFT of n-tuples over $Q(m,r)$ corresponding to the ideals of the ring

$$F[GZ_m] \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GR(p_i^{k_i}, e_{ij}).$$

Hence any Abelian code over Z_m is of the form

$$L \equiv \bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} p^{h_{ij}} GR(p_i^{k_i}, e_{ij}) \; ; \quad 0 \leq h_{ij} \leq k.$$

and it can be seen from the above expression that every Abelian code over Z_m is a direct sum of Abelian codes over $Z_{p_i^{k_i}}$, $i=1,2,\ldots,s$.

5.6 SEMI-SIMPLE ABELIAN CODES; $m = p_1p_2\ldots p_s$

When $m = p_1p_2\ldots p_s$, Z_m is a semi-simple ring. Let G be an Abelian group of order n and $(n,m)=1$. Then from Theorem 2.4, the group ring GZ_m is semi-simple. Hence every Abelian code over Z_m in this case has an idempotent generator.

All the results concerning semi-simple cyclic codes over Z_m are valid in the case of Abelian codes also. We give below these results stated for Abelian codes in two theorems. The proofs are not given since they are identical to the proofs of the corresponding theorems for cyclic codes except that for given n and m only the conjugacy classes are different.

Theorem 5.7: The subring $F[GZ_m]$ of $Q^n(m,r)$ which contains all the transform vectors of n-tuples over Z_m, $m = p_1p_2\ldots p_s$, is isomorphic to a direct sum of finite fields

$$\bigoplus_{i=1}^{s} \bigoplus_{j=1}^{t_i} GF(p_i^{e_{ij}})$$

where t_i is the number of conjugacy classes corresponding to p_i in the appropriate mixed-radix number system and e_{ij}, $j=1,2,\ldots,t_i$, are the exponents of the conjugacy classes.

Theorem 5.8 Every Abelian code over Z_m, $m = p_1p_2\ldots p_s$, is uniquely determined by a subset of idempotent elements of Z_m.

Example 5.5 Let us consider Abelian codes with symbols from Z_{10} and the noncyclic Abelian group of order 9. The conjugacy classes are

$C_{2,9}(\langle 00\rangle) = \{\langle 00\rangle\}$ $\quad$ $C_{5,9}(\langle 00\rangle) = \{\langle 00\rangle\}$

$C_{2,9}(\langle 01\rangle) = \{\langle 01\rangle,\langle 02\rangle\}$ $\quad$ $C_{5,9}(\langle 01\rangle) = \{\langle 01\rangle,\langle 02\rangle\}$

$C_{2,9}(\langle 10\rangle) = \{\langle 10\rangle,\langle 20\rangle\}$ $\quad$ $C_{5,9}(\langle 10\rangle) = \{\langle 10\rangle,\langle 20\rangle\}$

$C_{2,9}(\langle 11\rangle) = \{\langle 11\rangle,\langle 22\rangle\}$ $\quad$ $C_{5,9}(\langle 11\rangle) = \{\langle 11\rangle,\langle 22\rangle\}$

$C_{2,9}(\langle 12\rangle) = \{\langle 12\rangle,\langle 21\rangle\}$ $\quad$ $C_{5,9}(\langle 12\rangle) = \{\langle 12\rangle,\langle 21\rangle\}$

The extension ring is GR(9,2). The idempotent elements of Z_{10} are 0,1,5 and 6. Each conjugacy class can take any one of the four idempotent elements. Hence there are total $4^5 = 1024$ Abelian codes including the trivial codes. For minimal Abelian codes the idempotent generators in the transform domain are listed in Table 5.5. In Table 5.5, $a+bx \in GR(9,2)$ is denoted simply by ab.

Table 5.5: Idempotent generators in the transform domain corresponding to Example 5.5.

$E_{<00>}$	$E_{<01>}$	$E_{<02>}$	$E_{<10>}$	$E_{<11>}$	$E_{<12>}$	$E_{<20>}$	$E_{<21>}$	$E_{<22>}$
00	00	00	00	00	00	00	00	00
10	00	00	00	00	00	00	00	00
50	00	00	00	00	00	00	00	00
60	00	00	00	00	00	00	00	00
00	10	10	00	00	00	00	00	00
00	50	50	00	00	00	00	00	00
00	60	60	00	00	00	00	00	00
00	00	00	10	00	00	10	00	00
00	00	00	50	00	00	50	00	00
00	00	00	60	00	00	60	00	00
00	00	00	00	10	00	00	00	10
00	00	00	00	50	00	00	00	50
00	00	00	00	60	00	00	00	60
00	00	00	00	00	10	00	10	00
00	00	00	00	00	50	00	50	00
00	00	00	00	00	60	00	60	00

CHAPTER 6

DUAL CODES OVER Z_m

In this chapter dual codes of cyclic and Abelian codes over Z_m are discussed. Dual codes are useful in the study of weight enumeration of linear codes. When the symbol alphabet has the structure of a finite field, it is well known that the weight enumerators of a linear code and its dual code are related by MacWilliams identities [6].

Delsarte [41] has assumed the abelian group structure for symbol alphabet, and obtained linear codes called additive codes. For additive codes, he has defined a duality relation which reduces to the classical concept of linear codes over a prime field and has shown that the MacWilliams identities on the weight distribution are still satisfied.

It is to be noted that Z_m has the structure of an abelian group when addition alone is considered and hence linear codes over Z_m are a particular class of additive codes. For the case of codes over Z_m, it is shown that the duality relation of Delsarte for additive codes reduces to the familiar relation of dot product being equal to zero. Codes over Z_m being additive codes, MacWilliams identities are satisfied for dual codes of linear

codes over Z_m. We study dual codes of cyclic and Abelian codes over Z_m in the transform domain.

Dual codes of linear codes over Z_m are defined in Section 6.1. Dual code pairs are characterised in terms of their DFT coefficients for the case of cyclic codes in Section 6.2. Results of Section 6.2 are used to obtain transform domain characterisation of self-dual cyclic codes in Section 6.3. It is shown that when $m = p^k$ and n and m are relatively prime, self-dual cyclic codes do not exist if k is an odd integer. For the case of $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, self-dual cyclic codes do not exist if at least one of k_i's is odd. Dual code pairs for Abelian codes are identified in the transform domain in Section 6.4. Self-dual Abelian codes are discussed in Section 6.5.

6.1 DEFINITION OF DUAL CODES OF LINEAR CODES OVER Z_m

When the alphabet has the structure of an abelian group, the notion of additive codes and their dual codes is developed in [41] as follows:

Let G be an abelian group of exponent q and G^n denote the set of all n-tuples over G. i.e.,

$$G^n = \{ (a_0, a_1, \ldots, a_{n-1}) : a_i \in G, \; i=0,1,\ldots,(n-1) \}$$

Let $\hat{G}$ denote the group of characters of G. It is well known that

$\hat{G} \equiv G$. Let $\hat{g}_g$ denote the character corresponding to $g \in G$ under this isomorphism. For $a, b \in G^n$, where $a = (a_0, a_1, \ldots, a_{n-1})$ and $(b_0, b_1, \ldots, b_{n-1})$ the inner product of a and b, denoted by $\langle a,b \rangle$, is defined as $\langle a,b \rangle = \prod_{i=0}^{n-1} \hat{g}_{b_i}(a_i)$. Let H be a subgroup of G^n. H is called as additive code over G. The dual of H is defined as the set $H^d \in G^n$ given by $H^d = \{ b \in G^n : \langle a,b \rangle = 1 \text{ for all } a \in A \}$. H^d is a subgroup of G^n and $H^d \equiv G^n/H$. i.e., H^d is isomorphic to the factor group G^n/H. When q is prime, an additive code is merely a linear code over GF(q) and the dual is the classical one.

For the case of linear codes over Z_m, we consider the abelian group $(Z_m,+) = \{ 0,1,2,\ldots,i,\ldots.m-1 \}$. It can be seen that the group of characters of $(Z_m,+)$ is $\hat{G} = \{ \hat{g}_0, \hat{g}_1, \ldots, \hat{g}_{m-1} \}$, where $\hat{g}_i$, $i=0,1,\ldots,m-1$, is given by

$$\hat{g}_i(x) = \alpha^{ix} \quad \text{for } x \in Z_m$$

where α is an element of multiplicative order m, and the group operation in $\hat{G}$ is given by

$$\hat{g}_i \hat{g}_j = \hat{g}_{i+j(\text{mod } m)}.$$

Now for $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1}) \in Z_m$, the inner product of a and b is given by

$$\langle a,b \rangle = \prod_{i=0}^{n-1} \hat{g}_{b_i}(a_i) = \prod_{i=0}^{n-1} (\alpha^{b_i})^{a_i} = \alpha \exp\left(\sum_{i=0}^{n-1} a_i b_i \right)$$

Hence $\langle a,b \rangle = 1$ iff $\sum_{i=0}^{n-1} a_i b_i = 0$. This leads to the following definition of dual code of a linear code over Z_m.

Definition 6.1 Let C be a linear code over Z_m. Then its dual code, denoted by $C^{\perp}$, is defined as

$$C^{\perp} = \{ (b_0,b_1,\ldots,b_{n-1}) : \sum_{i=0}^{n-1} a_i b_i = 0 \text{ for all } (a_0,a_1,\ldots,a_{n-1}) \in C \}$$

Note that this definition is same as that for codes over finite fields.

In what follows, we discuss the dual codes of cyclic and Abelian codes over Z_m in the transform domain.

6.2 SPECTRAL CHARACTERISATION OF DUAL CODES OF CYCLIC CODES

In this section, characterisation of dual code pairs of cyclic codes over Z_m in the transform domain is obtained.

Let $m = p^k$ and let us call the conjugacy class $C_{p,n}(n-j)$ the dual conjugacy class of $C_{p,n}(j)$ and the ideal $p^{(k-j)}GR(p^k,r)$ of $GR(p^k,r)$ the orthogonal ideal of $p^jGR(p^k,r)$. Note that product of two elements, one each from $p^jGR(p^k,r)$ and $p^{(k-j)}GR(p^k,r)$, is zero. If I denotes an ideal of $GR(p^k,r)$ then I_d is used to denote the orthogonal ideal of I. Note that $I.I_d = 0$.

Theorem 6.1 Let $a = (a_0, a_1, \ldots, a_{n-1})$ and $b = (b_0, b_1, \ldots, b_{n-1})$ be codewords and $A = (A_0, A_1, \ldots, A_{n-1})$ and $B = (B_0, B_1, \ldots, B_{n-1})$ be their transform vectors. If $b_j = a_{n-j}$ for all $j=0,1,\ldots,(n-1)$, then $B_j = A_{(n-j)}$ for all $j=0,1,\ldots,(n-1)$.

Proof: Let α be the transform factor of the DFT.
For any $j \in \{ 0,1,2,\ldots,(n-1) \}$, we have

$$B_j = \sum_{i=0}^{n-1} \alpha^{ij} b_i = \sum_{i=0}^{n-1} \alpha^{ij} a_{n-i}$$

$$= \sum_{k=0}^{n-1} \alpha^{(n-k)j} a_k = \sum_{k=0}^{n-1} \alpha^{-kj} a_k \qquad \text{since } \alpha^n = 1.$$

and

$$A_{(n-j)} = \sum_{i=0}^{n-1} \alpha^{i(n-j)} a_i = \sum_{i=0}^{n-1} \alpha^{-ij} a_i = \sum_{k=0}^{n-1} \alpha^{-kj} a_k.$$

Hence $B_j = A_{(n-j)}$. Q.E.D.

In Theorem 6.1, $(b_0, b_1, \ldots, b_{n-1})$ is a permutation of $(a_0, a_1, \ldots, a_{n-1})$, the permutation being defined by $i \dashrightarrow (n-i)$. Theorem 6.1 shows that this permutation is preserved under DFT.

Theorem 6.2 If C is a cyclic code of length n over Z_{p^k} whose transform vectors take values from the ideals $I_1, I_2, \ldots, I_t$ for the conjugacy classes $C_{p,n}(j_1)$, $C_{p,n}(j_2)$, ..., $C_{p,n}(j_t)$ respectively then the transform vectors of the dual code $C^{\perp}$ take values from the ideals $(I_1)_d, (I_2)_d, \ldots, (I_t)_d$ respectively for the conjugacy classes $C_{p,n}(n-j_1)$, $C_{p,n}(n-j_2), \ldots, C_{p,n}(n-j_t)$.

Proof: Let $a = (a_0, a_1, \ldots, a_{n-1})$ be represented by $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1} = a(x)$ and let $a(x) \in C$. Let C^* denote the cyclic code with ideals $(I_1)_d$, $(I_2)_d$, $\ldots$, $(I_t)_d$ in the conjugacy classes $C_{p,n}(j_1)$, $C_{p,n}(j_2)$, $\ldots$, $C_{p,n}(j_t)$ and let $h(x) = h_0 + h_1 x + \ldots + h_{n-1}x^{n-1} \in C^*$. From the convolution property of DFT it is clear that $a(x)h(x) = 0$ for all $a(x) \in C$ and for all $h(x) \in C^*$. In particular, the constant term in the product $a(x)h(x)$ is zero. i.e., $\sum_{i=0}^{n-1} a_i h_{n-i} = 0$. For a given $h(x)$ in C^* define $b(x) = b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}$ by $b_i = h_{n-i}$, $i = 0, 1, \ldots, (n-1)$. We have $\sum_{i=0}^{n-1} a_i b_i = 0$. Hence $b(x)$ belongs to the dual code $C^{\perp}$. From Theorem 6.1, it follows that the transform vector of $b(x)$ have values from ideals $(I_1)_d$, $(I_2)_d$, $\ldots$, $(I_t)_d$ for the conjugacy classes $C_{p,n}(n-j_1)$, $C_{p,n}(n-j_2)$, $\ldots$, $C_{p,n}(n-j_t)$. So we have shown that the set of all $b(x)$ corresponding to all the elements of C^*, denoted by C^{**}, is contained in $C^{\perp}$. It remains to show that they are, in fact, all the codewords of $C^{\perp}$.

We know that $C^{\perp}$ is contained in $Z_{p^k}^n/C$, which is the factor group, considering both $Z_{p^k}^n$ and C as groups [42]. So, it is sufficient to show that

$$|C|\ |C^{**}| = (p^k)^n = p^{kn} \qquad (6.2.1)$$

where $|C|$ denotes the number of elements in C. Let I_u be the ideal $p^{i_u}GR(p^k, r)$ for some i_u, $0 \leq i_u \leq k$, for $u = 1, 2, \ldots, t$. Also let $e_1, e_2, \ldots, e_t$ be the exponents of $C_{p,n}(j_1)$, $C_{p,n}(j_2)$, $\ldots$, $C_{p,n}(j_t)$ respectively. Note that sum of the exponents of all the conjugacy classes, $e_1 + e_2 + \ldots + e_t$, is equal to n. Then

$$|C| = (p^{i_1})^{e_1} (p^{i_2})^{e_2} \ldots (p^{i_t})^{e_t}$$

$$= p^{i_1 e_1} p^{i_2 e_2} \ldots p^{i_t e_t}$$

Similarly

$$|C^{**}| = (p^{k-i_1})^{e_1} (p^{k-i_2})^{e_2} \ldots (p^{k-i_t})^{e_t} .$$

Hence L.H.S. of eq.(6.2.1) $= (p^k)^{(e_1+e_2+ \ldots +e_t)}$

$= p^{kn}$

= R.H.S. of eq.(6.2.1). Q.E.D.

6.3 SELF-DUAL CYCLIC CODES OVER Z_m

From Theorem 6.2, the following spectral characterisation of self-dual cyclic codes follows immediately.

Theorem 6.3: A code C is a self-dual cyclic code iff whenever $C_{p,n}(j)$ has values from the ideal I then $C_{p,n}(n-j)$ has values from the ideal I_d.

Example 6.1 Let n=3 and m=4. The appropriate extension ring is GR(4,2). The only ideal in it such that $I = I_d$ is 2GR(4,2). Both the conjugacy classes (0) and (1,2) are self-dual. So the only possible self-dual code in this case is the one with all the conjugacy classes taking values from the ideal 2GR(4,2). All the codewords and their transform vectors are shown in the next page.

codewords			transform vectors		
a_0	a_1	a_2	A_0	A_1	A_2
0	0	0	00	00	00
2	0	0	20	20	20
0	2	0	20	02	22
2	2	0	00	22	02
2	0	2	00	02	22
0	0	2	20	22	02
0	2	2	00	20	20
2	2	2	20	00	00

Example 6.2: Consider length 5 cyclic codes over Z_4. The conjugacy classes are {0} and {1,2,3,4}. Both are self-dual conjugacy classes. The extension ring is GR(4,4). The only self-orthogonal ideal is 2GR(4,4). Hence there is only one self-dual code in this case which is listed in Table 6.1.

Example 6.3 In this example we obtain all self-dual codes of length 7 over Z_4. The conjugacy classes are $C_{2,7}(0) = \{ 0 \}$, $C_{2,7}(1) = \{ 1,2,4 \}$ and $C_{2,7}(3) = \{ 3,5,6 \}$. The extension ring of Z_4 is GR(4,3). The ideals in GR(4,3) are 2^0GR(4,3), 2^1GR(4,3) and 2^2GR(4,3). The conjugacy class $C_{2,7}(3)$ is the dual conjugacy class of $C_{2,7}(1)$ and the dual conjugacy class of $C_{2,7}(0)$ is itself. Among the ideals of GR(4,3), 2^2GR(4,3) is the orthogonal ideal of 2^0GR(4,3) and 2^1GR(4,3) is a self orthogonal ideal. So for a self-dual cyclic code, the conjugacy class $C_{2,7}(0)$ has to take values from 2^1GR(4,3) and $C_{2,7}(1)$ can take values either from 2^0GR(4,3) in which case $C_{2,7}(3)$ take values from 2^2GR(4,3), or from 2^2GR(4,3) in which case $C_{2,7}(3)$ take values from 2^0GR(4,3), or from 2^1GR(4,3) in which case $C_{2,7}(3)$

Table 6.1 Self-dual code of length 5 over Z_4.

Codeword					Spectrum				
a_0	a_1	a_2	a_3	a_4	A_0	A_1	A_2	A_3	A_4
0	0	0	0	0	0000	0000	0000	0000	0000
2	0	0	0	0	2000	2000	2000	2000	2000
0	0	2	0	0	2000	2222	0202	0022	0002
2	2	2	0	0	2000	0200	0020	2020	2200
0	2	0	2	0	0000	0020	2200	0200	2020
2	0	2	2	0	2000	0220	2220	2220	0220
0	0	0	0	2	2000	0202	0002	2222	0022
2	2	0	0	2	2000	2220	0220	0220	2220
0	2	2	0	2	2000	2002	2022	2202	0222
2	0	0	2	2	2000	2200	2020	0020	0200
0	0	2	2	2	2000	2022	0222	2002	2202
2	2	2	2	2	2000	0000	0000	0000	0000
2	2	0	0	0	2000	0022	2222	0002	0202
2	0	2	0	0	0000	0222	2202	2022	2002
0	0	0	2	0	2000	0002	0022	0202	2222
2	2	0	2	0	2000	2020	0200	2200	0020
0	2	2	2	0	2000	2202	2002	0222	2022
2	0	0	0	2	0000	2202	2002	0222	2022
0	0	2	0	2	0000	2020	0200	2200	0020
2	2	2	0	2	0000	0002	0022	0202	2222
0	2	0	2	2	2000	0222	2202	2022	2002
2	0	2	2	2	0000	0022	2222	0002	0202
2	2	0	0	0	0000	2022	0222	2002	2202
0	2	2	0	0	0000	2200	2020	0020	0200
2	0	0	2	0	0000	2002	2022	2202	0222
0	0	2	2	0	0000	2220	0220	0220	2220
2	2	2	2	0	0000	0202	0002	2222	0022
0	2	0	0	2	0000	0220	2220	2220	0220
2	0	2	0	2	2000	0020	2200	0200	2020
0	0	0	2	2	0000	0200	0020	2020	2200
2	2	0	2	2	0000	2222	0202	0022	0002
0	2	2	2	2	0000	2000	2000	2000	2000

also take values from $2^1GR(4,3)$. So, totally there are three self-dual codes. A complete listing of all codewords of all the three self-dual codes of this example is given in Appendix B.

6.3.1 Non-existence theorems for cyclic self-dual codes

In this section non-existence theorems are given which identify a set of values of m and n for which self-dual codes do not exist.

Theorem 6.4: If $m = p^k$ and $(n,m) = 1$ then self-dual cyclic codes of length n over Z_m do not exist for all odd values of k.

Proof: For all values of m and n, (0) is the conjugacy class $C_{p,n}(0)$ and $C_{p,n}(n-0)$ is also (0). Considering the conjugacy class (0), from Theorem 6.2, it is necessary that for a code C to be self-dual there must be at least one ideal I in $GR(p^k,r)$ such that $I = I_d$, from which (0) can take values. i.e., it is required that at least for one value of j, we have $p^jGR(p^k,r) = p^{(k-j)}GR(p^k,r)$. This can happen only if $j = k-j$ or $k=2j$, an even number. Q.E.D.

The well known result that a binary self-dual cyclic code is always of even length follows from the above theorem.

For any arbitrary integer $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$ let $a = (a_0,a_1,\ldots,a_{n-1})$ and $b = (b_0,b_1,\ldots,b_{n-1}) \in Z_m^n$. Choose m_i's such that $m_im_j = 1(\text{mod } m)$ if $i = j$ and $m_im_j = 0(\text{mod } m)$ if $i \neq j$.

We have

$$a_i = (m_1 a_{i1} + m_2 a_{i2} + \ldots + m_s a_{is}) \bmod m$$

$$b_i = (m_1 b_{i1} + m_2 b_{i2} + \ldots + m_s b_{is}) \bmod m$$

where a_{ij} and $b_{ij} \in Z_{p_j^{k_j}}$ for $i,j=1,2,\ldots,s$. It can be verified that $\sum_{i=0}^{n-1} a_i b_i = 0$ iff $\sum_{i=0}^{n-1} a_{ij} b_{ij} = 0$ for $j=1,2,\ldots,s$. Combining this result with Theorem 4.5, Theorem 6.3 and Theorem 6.4, we obtain

Theorem 6.5: If $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$ and $(n,m)=1$ then self-dual codes of length n over Z_m do not exist if any one of k_i's is an odd number.

6.4 DUAL CODES OF ABELIAN CODES

In this section we characterise dual codes of Abelian codes in the transform domain.

It is assumed that $m = p^k$. Let us recall that $\langle j \rangle$ denotes the mixed-radix number in an appropriate mixed-radix number system and $C_{p,n}(\langle j \rangle)$ denotes the conjugacy class in that mixed-radix system containing $\langle j \rangle$. The conjugacy class $C_{p,n}(\langle n-j \rangle)$ is called the dual conjugacy class of $C_{p,n}(\langle j \rangle)$.

In the following theorem, we show that under the generalised DFT, the permutation of codeword symbols defined by $\langle i \rangle \longrightarrow \langle n-i \rangle$ is carried over to their DFT coefficients.

Theorem 6.6: Let $a = (a_{<0>}, a_{<1>}, \ldots, a_{<n-1>})$ and $b = (b_{<0>}, b_{<1>}, \ldots, b_{<n-1>})$ be codewords and $A = (A_{<0>}, A_{<1>}, \ldots, A_{<n-1>})$ and $B = (B_{<0>}, B_{<1>}, \ldots, B_{<n-1>})$ their transform vectors, where a_i, $b_i \in Z_{p^k}$ and A_i, $B_i \in GR(p^k, r)$, $i=0,1,\ldots,n-1$. If $a_{<i>} = b_{<n-i>}$ for $i=0,1,\ldots,n-1$, then $A_{<i>} = B_{<n-i>}$ for $i=0,1,\ldots,n-1$.

Proof: For any $j \in \{0,1,\ldots,n-1\}$, we have

$$B_{<j>} = \sum_{<i>=0}^{n-1} (\alpha_{n_0})^{i_0 j_0} (\alpha_{n_1})^{i_1 j_1} \ldots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}} \; b_{<i>}$$

$$= \sum_{<i>=0}^{n-1} (\alpha_{n_0})^{i_0 j_0} (\alpha_{n_1})^{i_1 j_1} \ldots (\alpha_{n_{v-1}})^{i_{v-1} j_{v-1}} \; a_{<n-i>}$$

(by putting $<n-i>=<k>$)

$$= \sum_{<k>=0}^{n-1} (\alpha_{n_0})^{j_0 (n_0 - k_0)} \ldots (\alpha_{n_{v-1}})^{j_{v-1} (n_{v-1} - k_{v-1})} \; a_{<k>}$$

and

$$A_{<n-j>} = \sum_{<i>=0}^{n-1} (\alpha_{n_0})^{i_0 (n_0 - j_0)} \ldots (\alpha_{n_{v-1}})^{i_{v-1} (n_{v-1} - j_{v-1})} \; a_{<n-i>}$$

(by putting $<k>=<n-i>$)

$$= \sum_{<k>=0}^{n-1} (\alpha_{n_0})^{-j_0 k_0} \ldots (\alpha_{n_{v-1}})^{-j_{v-1} k_{v-1}} \; a_{<k>}$$

$$= B_{<j>}$$ Q.E.D.

The following theorem characterises self-dual Abelian codes in the transform domain.

Theorem 6.7: If L is an Abelian code of length n over Z_{p^k} whose transform vectors take values from the ideals $I_1, I_2, \ldots, I_t$ for the conjugacy classes $C_{p,n}(<j_1>)$, $C_{p,n}(<j_2>)$, ..., $C_{p,n}(<j_t>)$

respectively then the transform vectors of the dual code $L^{\perp}$ take values from the ideals $(I_1)_d$, $(I_2)_d$,...,$(I_t)_d$ respectively for the conjugacy classes $C_{p,n}(\langle n-j_1\rangle)$, $C_{p,n}(\langle n-j_2\rangle)$,...,$C_{p,n}(\langle n-j_t\rangle)$.

Proof: Let $a = (a_{\langle 0\rangle}, a_{\langle 1\rangle}, \ldots, a_{\langle n-1\rangle}) \in L$. Let L' denote the Abelian code with ideals $(I_1)_d$, $(I_2)_d$,...,$(I_t)_d$ in the conjugacy classes $C_{p,n}(\langle j_1\rangle)$, $C_{p,n}(\langle j_2\rangle)$, ..., $C_{p,n}(\langle j_t\rangle)$. Let $h = (h_{\langle 0\rangle}, h_{\langle 1\rangle}, \ldots, h_{\langle n-1\rangle}) \in L'$. From $A_i H_i = 0$, $i = 0,1,\ldots,n-1$, where $A = (A_{\langle 0\rangle}, A_{\langle 1\rangle}, \ldots, A_{\langle n-1\rangle})$ and $H = (H_{\langle 0\rangle}, H_{\langle 1\rangle}, \ldots, H_{\langle n-1\rangle})$ are the transform vectors of a and h respectively, it follows that

$$\left(\sum_{\langle i\rangle=0}^{n-1} a_i g_i\right)\left(\sum_{\langle j\rangle=0}^{n-1} h_j g_j\right) = 0$$

where g_i, $i=0,1,\ldots,n-1$, are the elements of the Abelian group under consideration. In particular, we have the coefficient of g_0 (identity element), equal to zero. i.e.,

$$\sum_{\langle i\rangle=0}^{n-1} a_{\langle i\rangle}\, h_{\langle n-i\rangle} = 0.$$

For a given h in L', define $b = (b_{\langle 0\rangle}, b_{\langle 1\rangle}, \ldots, b_{\langle n-1\rangle})$, by $b_{\langle i\rangle} = h_{\langle n-i\rangle}$, $i=0,1,\ldots,n-1$. We have $\sum_{\langle i\rangle=0}^{n-1} a_{\langle i\rangle} b_{\langle i\rangle} = 0$. Hence $b \in L^{\perp}$. But from Theorem 6.6, it follows that the transform vector of b have values from ideals $(I_1)_d$, ...,$(I_t)_d$ for the conjugacy classes $C_{p,n}(\langle n-j_1\rangle)$, ..., $C_{p,n}(\langle n-j_t\rangle)$. So we have shown that the set of all b corresponding to all elements of L', denoted by L'', is contained in $L^{\perp}$. We proceed to show that $L^{\perp}$ is nothing but L''.

It is known that $L^{\perp}$ is contained in Z_{pk}^{n}/L. So it is

sufficient to show that

$$|L|\ |L''| = (p^k)^n = p^{kn} .$$

Let I_u be the ideal $p^{i_u}GR(p^k,r)$, for some $0 \leq i_u \leq k$, for $u=1,2,\ldots,t$. Let $e_1,e_2,\ldots,e_t$ be the exponents of the conjugacy classes $C_{p,n}(\langle j_1\rangle)$, $C_{p,n}(\langle j_2\rangle)$, ..., $C_{p,n}(\langle j_t\rangle)$. We have

$$\begin{aligned} |L| &= (p^{i_1})^{e_1}\ (p^{i_2})^{e_2}\ \ldots\ldots\ (p^{i_t})^{e_t} \\ &= p^{i_1e_1}\ p^{i_2e_2}\ \ldots\ldots\ p^{i_te_t} \\ &= p^{i_1e_1 + i_2e_2 + \ldots\ldots + i_te_t} \end{aligned}$$

Similarly

$$|L''| = p^{(k-i_1)e_1 + (k-i_2)e_2 + \ldots + (k-i_t)e_t}$$

Hence

$$\begin{aligned} |L|\ |L''| &= (p^k)^{e_1+e_2+\ \ldots\ +e_t} \\ &= p^{kn}. \end{aligned}$$

Q.E.D.

6.5 SELF-DUAL ABELIAN CODES

In this section a simple transform domain characterisation of self-dual Abelian codes is given and results regarding non-existence of self-dual Abelian codes are obtained in similar lines to those obtained for cyclic codes in Section 6.4.

Transform domain characterisation of self-dual Abelian codes follows from Theorem 6.7 as given below.

Theorem 6.8: An Abelian code A is self-dual iff whenever $C_{p,n}(\langle j \rangle)$ has values from the ideal I, $C_{p,n}(\langle n-j \rangle)$ has values from the ideal I_d.

6.5.1 Non-existence theorems for self-dual Abelian codes

Theorem 6.9: If $m = p^k$ and $(n,m) = 1$, then self-dual Abelian codes of length n over Z_m do not exist if k is odd.

Proof: For all values of m and n, (0) is a conjugacy class and its dual conjugacy class is same. From Theorem 6.8, it follows that for an Abelian code L to be self-dual there must be an ideal I in $GR(p^k,r)$ such that $I = I_d$, since only elements from such an ideal can occupy the conjuacy class (0). If $I = p^j GR(p^k,r)$ then $I_d = p^{k-j}GR(p^k,r)$. For $I = I_d$ to hold true, it is required that $p^jGR(p^k,r) = p^{k-j}GR(p^k,r)$. In other words $p^j = p^{k-j}$ or $j = k-j$, i.e., $k = 2j$ an even number. Q.E.D.

For arbitrary integer $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, it is easy to check that, the arguments similar to those given to obtain Theorem 6.5 for the case of cyclic codes holds true for the case of Abelian codes also and hence we have the following theorem.

Theorem 6.10: If $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$ and $(n,m) = 1$ then self-dual Abelian codes of length n over Z_m do not exist if at least one of k_i's is an odd integer.

CHAPTER 7

DECODING ALGORITHM FOR BCH CODES OVER Z_m

In this chapter we describe a decoding algorithm for BCH codes over Z_m which are defined in the transform domain by zeros in the consecutive spectral components. The decoding algorithm described is precisely for the BCH codes described by Prithi Shankar in terms of generator polynomials [12].

The equivalence of the decoding problem of BCH codes over finite fields to a shift register synthesis problem is well known [32]. In Section 7.1, it is shown that the problem of decoding BCH codes over Z_{p^k} is equivalent to the problem of shift register synthesis over Galois rings. An algorithm for linear feedback shift register synthesis over Z_{p^k} is given by Reeds and Sloane in [44]. In Section 7.2, we show that this algorithm, with minor modification, is valid for synthesising linear feedback shift register over Galois rings. A sample computation of BCH decoding algorithm is described, in Section 7.3.

Without loss of generality it is assumed that $m = p^k$. We recall that in general a BCH code of length n over Z_{p^k} consists of the inverse discrete Fourier transform of all vectors whose d consecuti DFT coefficients are from the same ideal. When the consecutive spectral components are zeros, say 2t consecutive

components, the Hamming distance of the code is at least 2t+1 and hence the code corrects upto t errors [12, Theorem 4]. For decoding we consider only these codes.

We consider an example of BCH code before describing the decoding algorithm.

Example 7.1: Let us construct a double error correcting BCH code over Z_9 of length 8. The appropriate extension ring is GR(9,2). The conjugacy classes are (0), (1,3), (2,6), (4) and (5,7). The transform matrix is given by

$$\begin{bmatrix}
10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\
10 & 31 & 75 & 28 & 80 & 68 & 24 & 71 \\
10 & 75 & 80 & 24 & 10 & 75 & 80 & 24 \\
10 & 28 & 24 & 31 & 80 & 71 & 75 & 68 \\
10 & 80 & 10 & 80 & 10 & 80 & 10 & 80 \\
10 & 68 & 75 & 71 & 80 & 31 & 24 & 28 \\
10 & 24 & 80 & 75 & 10 & 24 & 80 & 75 \\
10 & 71 & 24 & 68 & 80 & 28 & 75 & 31
\end{bmatrix}$$

Each entry ab represents a+bx, an element of GR(9,2). The transform factor is 3+x. The automorphism defining conjugacy constraint is $\sigma(x) = 8+8x$.

For double error correction four consecutive zeros are sufficient. However we take first five DFT coefficients zeros.

Table 7.1 Codewords and spectrum of double error correcting BCH code over Z_9 of length 8.

Codeword								Spectrum							
a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	A_0	A_1	A_2	A_3	A_4	A_5	A_6	A_7
0	0	0	0	0	0	0	0	00	00	00	00	00	00	00	00
0	1	5	8	0	8	4	1	00	00	00	00	00	51	00	48
0	2	1	7	0	7	8	2	00	00	00	00	00	12	00	87
0	3	6	6	0	6	3	3	00	00	00	00	00	63	00	36
0	4	2	5	0	5	7	4	00	00	00	00	00	24	00	75
0	5	7	4	0	4	2	5	00	00	00	00	00	75	00	24
0	6	3	3	0	3	6	6	00	00	00	00	00	36	00	63
0	7	8	2	0	2	1	7	00	00	00	00	00	87	00	12
0	8	4	1	0	1	5	8	00	00	00	00	00	48	00	51
1	0	1	5	8	0	8	4	00	00	00	00	00	52	00	37
1	1	6	4	8	8	3	5	00	00	00	00	00	13	00	76
1	2	2	3	8	7	7	6	00	00	00	00	00	64	00	25
1	3	7	2	8	6	2	7	00	00	00	00	00	25	00	64
1	4	3	1	8	5	6	8	00	00	00	00	00	76	00	13
1	5	8	0	8	4	1	0	00	00	00	00	00	37	00	52
1	6	4	8	8	3	5	1	00	00	00	00	00	88	00	01
1	7	0	7	8	2	0	2	00	00	00	00	00	40	00	40
1	8	5	6	8	1	4	3	00	00	00	00	00	01	00	88
2	0	2	1	7	0	7	8	00	00	00	00	00	14	00	65
2	1	7	0	7	8	2	0	00	00	00	00	00	65	00	14
2	2	3	8	7	7	6	1	00	00	00	00	00	26	00	53
2	3	8	7	7	6	1	2	00	00	00	00	00	77	00	02
2	4	4	6	7	5	5	3	00	00	00	00	00	38	00	41
2	5	0	5	7	4	0	4	00	00	00	00	00	80	00	80
2	6	5	4	7	3	4	5	00	00	00	00	00	41	00	38
2	7	1	3	7	2	8	6	00	00	00	00	00	02	00	77
2	8	6	2	7	1	3	7	00	00	00	00	00	53	00	26
3	0	3	6	6	0	6	3	00	00	00	00	00	66	00	03
3	1	8	5	6	8	1	4	00	00	00	00	00	27	00	42
3	2	4	4	6	7	5	5	00	00	00	00	00	78	00	81
3	3	0	3	6	6	0	6	00	00	00	00	00	30	00	30
3	4	5	2	6	5	4	7	00	00	00	00	00	81	00	78
3	5	1	1	6	4	8	8	00	00	00	00	00	42	00	27
3	6	6	0	6	3	3	0	00	00	00	00	00	03	00	66
3	7	2	8	6	2	7	1	00	00	00	00	00	54	00	15
3	8	7	7	6	1	2	2	00	00	00	00	00	15	00	54
4	0	4	2	5	0	5	7	00	00	00	00	00	28	00	31
4	1	0	1	5	8	0	8	00	00	00	00	00	70	00	70
4	2	5	0	5	7	4	0	00	00	00	00	00	31	00	28
4	3	1	8	5	6	8	1	00	00	00	00	00	82	00	67
4	4	6	7	5	5	3	2	00	00	00	00	00	43	00	16
4	5	2	6	5	4	7	3	00	00	00	00	00	04	00	55
4	6	7	5	5	3	2	4	00	00	00	00	00	55	00	04
4	7	3	4	5	2	6	5	00	00	00	00	00	16	00	43
4	8	8	3	5	1	1	6	00	00	00	00	00	67	00	82

5	0	5	7	4	0	4	2	00	00	00	00	00	71	00	68
5	1	1	6	4	8	8	3	00	00	00	00	00	32	00	17
5	2	6	5	4	7	3	4	00	00	00	00	00	83	00	56
5	3	2	4	4	6	7	5	00	00	00	00	00	44	00	05
5	4	7	3	4	5	2	6	00	00	00	00	00	05	00	44
5	5	3	2	4	4	6	7	00	00	00	00	00	56	00	83
5	6	8	1	4	3	1	8	00	00	00	00	00	17	00	32
5	7	4	0	4	2	5	0	00	00	00	00	00	68	00	71
5	8	0	8	4	1	0	1	00	00	00	00	00	20	00	20
6	0	6	3	3	0	3	6	00	00	00	00	00	33	00	06
6	1	2	2	3	8	7	7	00	00	00	00	00	84	00	45
6	2	7	1	3	7	2	8	00	00	00	00	00	45	00	84
6	3	3	0	3	6	6	0	00	00	00	00	00	06	00	33
6	4	8	8	3	5	1	1	00	00	00	00	00	57	00	72
6	5	4	7	3	4	5	2	00	00	00	00	00	18	00	21
6	6	0	6	3	3	0	3	00	00	00	00	00	60	00	60
6	7	5	5	3	2	4	4	00	00	00	00	00	21	00	18
6	8	1	4	3	1	8	5	00	00	00	00	00	72	00	57
7	0	7	8	2	0	2	1	00	00	00	00	00	85	00	34
7	1	3	7	2	8	6	2	00	00	00	00	00	46	00	73
7	2	8	6	2	7	1	3	00	00	00	00	00	07	00	22
7	3	4	5	2	6	5	4	00	00	00	00	00	58	00	61
7	4	0	4	2	5	0	5	00	00	00	00	00	10	00	10
7	5	5	3	2	4	4	6	00	00	00	00	00	61	00	58
7	6	1	2	2	3	8	7	00	00	00	00	00	22	00	07
7	7	6	1	2	2	3	8	00	00	00	00	00	73	00	46
7	8	2	0	2	1	7	0	00	00	00	00	00	34	00	85
8	0	8	4	1	0	1	5	00	00	00	00	00	47	00	62
8	1	4	3	1	8	5	6	00	00	00	00	00	08	00	11
8	2	0	2	1	7	0	7	00	00	00	00	00	50	00	50
8	3	5	1	1	6	4	8	00	00	00	00	00	11	00	08
8	4	1	0	1	5	8	0	00	00	00	00	00	62	00	47
8	5	6	8	1	4	3	1	00	00	00	00	00	23	00	86
8	6	2	7	1	3	7	2	00	00	00	00	00	74	00	35
8	7	7	6	1	2	2	3	00	00	00	00	00	35	00	74
8	8	3	5	1	1	6	4	00	00	00	00	00	86	00	23

The conjugacy classes which take zero are (0), (1,3), (2,6) and (4). The only other conjugacy class (5,7) take values from the full ring GR(9,2). A complete listing of all the codewords with their DFT coefficients is given in Table 7.1.

7.1 EQUIVALENCE OF DECODING BCH CODES AND SHIFT REGISTER SYNTHESIS OVER GALOIS RING

In this section we show that the problem of decoding BCH codes with consecutive zeros in the spectral components is equivalent to minimal feed-back shift register synthesis problem over Galois rings.

The BCH codes under consideration for decoding are t error-correcting of length n and without loss of generality, it is assumed that the first 2t consecutive DFT coefficients are zeros.

Let us associate with an n-tuple $a = (a_0, a_1, \ldots, a_{n-1})$ over Z_{p^k} the polynomial

$$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \in Z_{p^k}[x]$$

Let $c = (c_0, c_1, \ldots, c_{n-1})$ be the transmitted codeword and $r = (r_0, r_1, \ldots, r_{n-1})$ and $e = (e_0, e_1, \ldots, e_{n-1})$ be the received and error vectors respectively. The associated polynomials are

$$c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}$$

$$r(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{n-1} x^{n-1}$$

$$e(x) = e_0 + e_1 x + e_2 x^2 + \ldots + e_{n-1} x^{n-1}$$

Assuming that only $\delta \leq t$ errors have occurred, we have only δ non-zero coefficients in e(x). Let

$$e(x) = e_{i_1}x^{i_1} + e_{i_2}x^{i_2} + \ldots + e_{i_\delta}x^{i_\delta}.$$

$i_1, i_2, \ldots, i_\delta$ be the locations of the errors and $e_{i_1}, e_{i_2}, \ldots, e_{i_\delta}$ be the magnitudes of the errors. Both locations and magnitudes are unknown. The decoding problem is finding these. Instead of finding error locations and magnitudes which means finding e(x), we obtain the transform vector of e(x), inverse DFT of which gives e(x) straightaway.

Let α be the transform factor of the DFT. We define S_j (the j-th syndrome) as $S_j = r(\alpha^j)$. Note that S_j is nothing but j-th DFT coefficient of the received vector. Since $r(x) = c(x)+e(x)$ and $c(x) = 0$ for $x = 0, 1, \ldots 2t-1$, the syndromes contain information due to errors only. i.e., the first 2t DFT coefficients of the error vector are equal to the syndromes $S_0, S_1, \ldots, S_{2t-1}$. So our aim is to obtain e(x) such that δ, the degree of e(x) is minimum and also has the first 2t DFT coefficients equal to syndromes.

Let us define the polynomial A(x), called error locator polynomial, by

$$A(x) = (1-x\alpha^{i_1})(1-x\alpha^{i_2}) \ldots (1-x\alpha^{i_\delta}).$$

The degree of A(x) is δ, which is atmost t, and A(x) is a

polynomial with coefficients in $GR(p^k,r)$. Let

$$A(x) = 1+A_1x+A_2x^2+ \ldots +A_{n-1}x^{n-1}.$$

The inverse DFT of A(x) is given by $A(\alpha^{-j})$, $j=0,1,\ldots,(n-1)$, which is same as A(x) evaluated at α^{-j}. We denote this inverse DFT of A(x) by $\Gamma = (\Gamma_0, \Gamma_1, \ldots, \Gamma_{n-1})$. Note that Γ is an n-tuple over $GR(p^k,r)$. Since A(x), in general, does not satisfy the conjugacy constraints inverse DFT is not an n-tuple over Z_{p^k}. By the definition of A(x), $A(\alpha^{-j})$ equals to zero if and only if j is an error location. Thus A(x) has been defined in such a way that in Γ, $\Gamma_i=0$ for all those i for which $e_i\neq 0$. Hence $\Gamma_i e_i=0$ for all $i=0,1,\ldots,(n-1)$. By the convolution property of the DFT, the convolution of transform vector of Γ and the transform vector of error vector, denoted by $E=(E_0,E_1,\ldots,E_{n-1})$, is equal to zero vector. That is,

$$\sum_{i=0}^{n-1} A_i E_{k-i} = 0 \qquad k=0,1,\ldots,(n-1).$$

Because A(x) has degree equal to δ, we have $A_j=0$ for $j>\delta$. Therefore

$$\sum_{i=0}^{\delta} A_i E_{k-i} = 0 , \qquad k=0,1,\ldots,(n-1).$$

Since $A_0=1$, we have

$$E_k = -\sum_{i=1}^{\delta} A_i E_{k-i} , \qquad k=0,1,\ldots,(n-1).$$

The coefficients A_i, $i=1,2,\ldots,\delta$, are unknown and among the n components of E only 2t are known which are equal to syndromes.

Thus

$$S_k = -\sum_{i=1}^{\delta} A_i S_{k-i}, \qquad k = \delta, \delta+1, \ldots, 2t-1 \quad (7.1.2)$$

involve only the known syndromes and the δ unknown components of A. From (7.1.2), it follows that the problem of obtaining $A_0, A_1, A_2, \ldots, A_\delta$ is nothing but synthesizing the minimal feedback shift register with tap coefficients $A_0, A_1, \ldots, A_\delta$ that generates the sequence $S_0, S_1, \ldots, S_{2t-1}$. Note that $S_0, S_1, \ldots, S_{2t-1}$ and $A_0, A_1, \ldots, A_\delta$ belong to a Galois ring and the requirement of minimising δ is taken care of since the synthesis is for the minimal length shift register. The problem of decoding BCH codes over Z_m is accordingly equivalent to the minimal shift register synthesis problem over Galois ring. By recursive extension, using (7.1.2), S_{2t}, S_{2t+1}, S_{2t+2}, ..., S_{n-1} can be obtained and inverse Fourier transform of $(S_0, S_1, S_2, \ldots, S_{n-1})$ straight away gives the error vector $(e_0, e_1, e_2, \ldots, e_{n-1})$.

7.2 AN ALGORITHM FOR SHIFT REGISTER SYNTHESIS OVER GALOIS RINGS

Now we proceed to describe the shift register synthesis algorithm over a Galois ring.

For Z_{p^k}, the minimal shift register algorithm has been obtained by Reeds and Sloane [44]. In this section we show that this algorithm, with minor modification, is valid for minimal shift register systhesis over Galois rings also. Our presentation of the algorithm is very similar to that of Reeds-Sloane and

familiarity with [44] will be of great use in following the algorithm.

The property of the Galois rings, stated in Fact 2.6, is the only idea that is required to know, apart from Reeds-Sloane's algorithm of shift register synthesis over Z_m, to get an algorithm that works over Galois ring. We recall, Fact 2.6, that in the Galois ring $GR(p^k,r)$ any non-zero element can be written as θp^t where u is a unit and $0 \leq t \leq k-1$ and in this representation the integer t is unique and θ is unique modulo (p^{k-t}). Note that this property holds for Z_{p^k} since Z_{p^k} is nothing but the Galois ring $GR(p^k,1)$.

Example 7.2: In Example 2.1 we have shown all the elements of $GR(4,2)$ in the form θp^t. Consider $GR(9,2) \equiv Z_9[x]/(x^2+x+2)$. Any element Γ of $GR(9,2)$ is of the form $a+bx$ where $a,b \in Z_9$; it is denoted by ab.In this example we express all the elements of $GR(9,2)$ in the form θp^t, in Table 7.2. This will be useful in the computation of the decoding algorithm for the BCH code given in Example 7.1.

Let $GR^*(p^e,r)$ denote the set of all units of the Galois ring $GR(p^e,r)$. The sequence $S_0,S_1,\ldots,S_{n-1}$ where $S_i \in GR(p^e,r)$, $i=1,2,\ldots,n-1$, is said to be generated by a linear feedback shift register of length δ if there are elements $a_0 = 1,a_1,a_2,\ldots,a_\delta \in GR(p^e,r)$ such that

Table 7.2 All elements of GR(9,2) corresponding to Example 7.2.

Γ	t	θ	$\theta \pmod{3^{(2-t)}}$	Γ	t	θ	$\theta \pmod{3^{(2-t)}}$
01	0	01	01	45	0	45	45
02	0	02	02	46	0	46	46
03	1	01,04,07	01	47	0	47	47
04	0	04	04	48	0	48	48
05	0	05	05	50	0	50	50
06	1	02,05,08	02	51	0	51	51
07	0	07	07	52	0	52	52
08	0	08	08	53	0	53	53
10	0	10	10	54	0	54	54
11	0	11	11	55	0	55	55
12	0	12	12	56	0	56	56
13	0	13	13	57	0	57	57
14	0	14	14	58	0	58	58
15	0	15	15	60	1	20,50,80	20
16	0	16	16	61	0	61	61
17	0	17	17	62	0	62	62
18	0	18	18	63	1	21,54,87	21
20	0	20	20	64	0	64	64
21	0	21	21	65	0	65	65
22	0	22	22	66	1	22,55,88	22
23	0	23	23	67	0	67	67
24	0	24	24	68	0	68	68
25	0	25	25	70	0	70	70
26	0	26	26	71	0	71	71
27	0	27	27	72	0	72	72
28	0	28	28	73	0	73	73
30	1	10,40,70	10	74	0	74	74
31	0	31	31	75	0	75	75
32	0	32	32	76	0	76	76
33	1	11,44,77	11	77	0	77	77
34	0	34	34	78	0	78	78
35	0	35	35	80	0	80	80
36	1	12,45,78	12	81	0	81	81
37	0	37	37	82	0	82	82
38	0	38	38	83	0	83	83
40	0	40	40	84	0	84	84
41	0	41	41	85	0	85	85
42	0	42	42	86	0	86	86
43	0	43	43	87	0	87	87
44	0	44	44	88	0	88	88

$$\sum_{i=0}^{\delta} a_i S_{j-i} = 0 \qquad \text{for } j=\delta,\delta+1,\ldots,(n-1) \qquad (7.2.1)$$

Let $a(x) = a_0+a_1x+a_2x^2+ \ldots +a_\delta x^\delta$ and $S(x) = S_0+S_1x+S_2x^2+\ldots\ldots +S_{n-1}x^{n-1}$. Clearly $a(x)$ and $S(x) \in GR(p^e,r)[x]$. Then (7.2.1) can be written as

$$S(x)a(x) = b(x) \pmod{x^n} ; \quad a(0) = 1 \qquad (7.2.2)$$

for some polynomial $b(x) \in GR(p^e,r)[x]$ of degree $\leq \delta-1$. Thus the length of the shift register is $\delta = \max \{ \deg a(x), 1+\deg b(x) \}$. We write $A = (a(x),b(x))$ and define

$$L(A) = \max \{ \deg a(x), 1+\deg b(x) \}.$$

By convention $\deg(0) = -\infty$.

7.2.1 THE ALGORITHM:

Let $S_0,S_1,\ldots,S_{n-1} \in GR(p^e,r)$. Our aim is to find $A = (a(x),b(x))$ of minimal length $\delta = L(A)$ satisfying eq (7.2.2). The following more general problem is considered. For all $i=0,1,2,\ldots,(e-1)$, find pairs $A_i = (a_i(x),b_i(x))$ such that

$$S(x)a_i(x) = b_i(x) \pmod{x^n}; \quad a_i(0) = p^i \qquad (7.2.3)$$

and $L(A_i) = \delta_i$ is minimised. This algorithm is an iterative procedure that for all $0 \leq k \leq n$, $0 \leq i \leq e$ calculates the pairs

$$A_i^{(k)} = (a_i^{(k)}(x), b_i^{(k)}(x))$$

satisfying

$$S(x)a_i^{(k)}(x) = b_i^{(k)}(x) \ (\mathrm{mod} x^k); \qquad a_i^{(k)}(0) = p^i$$

and minimising $L(A_i(k))$. Let $p^{t_{ik}}$ $(0 \leq t_{ik} \leq e)$ be the highest power of p dividing the coefficient of x^k in

$$S(x)a_i^{(k)}(x) - b_i^{(k)}(x)$$

($t_{ik} = e$ if the coefficient of x^k is zero). Then at the k-th step in the iteration, the following property holds for all $0 \leq j \leq k$. For all $0 \leq g < e$, either

$$L(A_g^{(j+1)}) = L(A_g^{(j)}) \qquad (7.2.4)$$

or else there exists $h = f(g,j)$ with

$$g + t_{hj} < e \qquad (7.2.5)$$

$$L(A_g^{(j+1)}) = j+1-L(a_h^{(j)}) \qquad (7.2.6)$$

$$L(A_g^{(j+1)}) > L(A_g^{(j)}) \qquad (7.2.7)$$

This property is analogous to the condition that Massey gives in [43, p.123, eqns (11)-(13)] for the finite field case. Given this data our algorithm calculates $A_i^{(k+1)}$ and $f(i,k)$, $0 \leq i < e$, such that property (P_k) holds. The quantities $L(A_i^{(k)})$ also obey the inequality

$$L(A_{i+1}^{(k)}) \leq L(A_i^{(k)}) \leq L(A_i^{(k+1)}).$$

Step 0: We start the algorithm with k=0 and for each i=0,1,...,e-1, define

$$a_i^{(0)}(x) = p^i, \quad b_i^{(0)}(x) = 0; \quad a_i^{(1)}(x) = p^i, \quad b_i^{(1)}(x) = p^i S_0$$

and $A_i^{(0)} = (a_i^{(0)}(x), b_i^{(0)}(x))$, $A_i^{(1)} = (a_i^{(1)}(x), b_i^{(1)}(x))$.

Let $S_0 = Up^t$ for $U \in GR^*(p^e,r)$, $0 \le t \le e$. (if $S_0=0$, set $U=1$ and $t=e$). Then

$$L(A_i^{(0)}) = 0$$

and

$$L(A_i^{(1)}) = 1 \quad \text{if} \quad i+t < e$$
$$= 0 \quad \text{if} \quad i+t \ge e.$$

We also define

$$u_{i0} = U, \; t_{i0} = i+t \qquad \text{if } i+t < e$$
$$u_{i0} = 1, \; t_{i0} = e \qquad \text{if } i+t \ge e$$

Finally we set $f(i,0) = 0$ for all i.

The following step is carried out for each $k=1,2,\ldots,(n-1)$.

Step k: This produces $A_i^{(k+1)}$. For each $i=0,1,..,(e-1)$, we perform the following calculations. Define $u_{ik} \in GR^*(p^e,r)$ and t_{ik}, $0 \le t_{ik} \le e$, by

$$S(x)a_i^{(k)}(x) = b_i^{(k)}(x) + u_{ik}\, p^{t_{ik}}\, x^k \pmod{x^{k+1}} \qquad (7.2.8)$$

($u_{ik}\, p^{t_{ik}}$ is the current discrepency in the notation of [43]).

Case I: If $t_{ik} = e$, set $A_i^{(k+1)} = A_i^{(k)}$.

Case II: If $t_{ik} < e$, define

$$g = e-1-t_{ik} \tag{7.2.9}$$

so that $0 \leq g < e$ and put

$$f(i,k) = g \tag{7.2.10}$$

There are now two subcases.

Case II(a): If $L(A_g^{(k)}) = 0$ we set

$$A_i^{(k+1)} = A_i^{(k)} + (0, u_{ik}\, p^{t_{ik}}\, x^k) \tag{7.2.11}$$

Case II(b): If $L(A_g^{(k)}) > 0$, then for some $0 \leq v < k$ we have

$$L(A_g^{(v)}) < L(A_g^{(v+1)}) = L(A_g^{(k)}) \tag{7.2.12}$$

v is the time of the most recent length change in the sequence $L(A_g^{(0)})$, $L(A_g^{(1)})$,.... From (7.2.5), (7.2.6) and (7.2.12) it follows that

$$L(A_g^{(k)}) = L(A_g^{(v+1)}) = v+1-L(A_h^{(v)}) \tag{7.2.13}$$

where

$$h = f(g,v) \quad \text{and} \quad g+t_{hv} < e. \tag{7.2.14}$$

From (7.2.9) and (7.2.14) we have $t_{hv} \leq t_{ik}$. Thus the power of p from the past can be used to annihilate the power of p in the current discrepency and we define

$$a_i^{(k+1)}(x) = a_i^{(k)}(x) - u_{ik}\, u_{hv}^{-1}\, p^{t_{ik}-t_{hv}}\, x^{k-v}\, a_h^{(v)}(x) \qquad (7.2.15)$$

$$b_i^{(k+1)}(x) = b_i^{(k)}(x) - u_{ik}\, u_{hv}^{-1}\, p^{t_{ik}-t_{hv}}\, x^{k-v}\, b_h^{(v)}(x) \qquad (7.2.16)$$

and $A_i^{(k+1)} = (a_i^{(k+1)}(x),\ b_i^{(k+1)}(x))$.

Then $S(x)\, a_i^{(k+1)}(x) = b_i^{(k+1)}(x) \pmod{x^{k+1}}$

and $a_i^{(k+1)}(0) = p^i$.

This concludes step k.

At the end of step (n-1) the algorithm terminates and the desired pair A = (a(x), b(x)) is given by

$$A_0^{(n)} = (a_0^{(n)}(x),\ b_0^{(n)}(x)).$$

The proof for the correctness of this algorithm is given in the following subsection.

7.2.2 Proof of correctness of the algorithm

Define

$$E_i^{(k)} = \{\ (a(x),b(x)) : S(x)a(x) = b(x) \pmod{x^k} \text{ and } a(0) = p^i\ \}$$

$$B_i^{(k)} = \{\ (a(x),b(x)) : S(x)a(x) = b(x) + u\, p^i\, x^k \pmod{x^{k+1}}\}$$

for $0 \le i < e$. Note that, if $(a(x),b(x)) \in E_i^{(k)}$ then $(pa(x),pb(x)) \in E_{i+1}^{(k)}$ and $(a(x),b(x))$ is in $B_i^{(k)}$ for some i,

$0 \leq i \leq e$, while if $i=e$ then $(a(x),b(x)) \in E_i^{(k+1)}$. Further, from (7.2.8), we have

$$A_i^{(k)} \in E_i^{(k)} \cap B_{t_i}^{(k)} \qquad (7.2.17)$$

Lemma 7.1: If $(a(x),b(x)) \in E_i^{(k)}$ and $(c(x),d(x)) \in B_v^{(k+1)}$ where $i+v < e$, then

$$L(a(x),b(x))+L(c(x),d(x)) \geq k \qquad (7.2.18)$$

Proof: Working modulo x^k we have

$$S(x)a(x) = b(x); \quad S(x)c(x) = d(x)+up^v s^{k-1} \text{ for } u \in GR^*(p^e,r),$$

so

$$\begin{aligned} b(x)c(x)-a(x)d(x) &= up^v x^{k-1} a(x) = up^v x^{k-1} a(0) \\ &= u\, p^{i+v} x^{k-1} \end{aligned} \qquad (7.2.19)$$

which does not vanish. Therefore the degree of the LHS of (7.2.19) is at least k-1. But

$$\begin{aligned} \deg(b(x)c(x)-a(x)d(x)) &\leq \max \{ \deg(b(x)c(x), \deg(a(x)d(x)) \} \\ &\leq L(a(x),b(x))+L(c(x),d(x))-1 \end{aligned}$$

as required. Q.E.D.

Definition 7.2: A pair $(a(x),b(x))$ is said to have minimal length in $E_i^{(k)}$ if $(a(x),b(x)) \in E_i^{(k)}$ and if

$$L(a(x),b(x)) \leq L(a'(x),b'(x)) \qquad (7.2.20)$$

holds for all $(a'(x),b'(x)) \in E_i^{(k)}$.

Lemma 7.2: Suppose in addition to the hypothesis of lemma 7.1 that equality holds in (7.2.18). Then (a(x),b(x)) has minimal length in $E_i^{(k)}$.

Proof: It immediately follows from Lemma 7.1. Q.E.D.

Theorem 7.1: For all k=0,1,...,n and i=0,1,...,e-1, A_i has minimal length in $E_i^{(k)}$.

Proof: The proof is by induction on k. The induction hypothesis is that when beginning step k, properties $P_0,P_1,..,P_{k-1}$ hold and $A_g^{(t)}$ has minimal length in $E_g^{(t)}$ for $0 \leq t \leq k$, $0 \leq g < e$. In step k, we compute t_{ik} from (7.2.8) and from $A_i^{(k+1)}$. To establish the induction we must show that at the end of step k, property P_k holds. i.e.,

(Pk): For all $0 \leq i < e$, either

$$L(A_i^{(k+1)}) = L(A_i^{(k)}) \qquad (7.2.21)$$

or else

$$i+t_{gk} < e \qquad (7.2.22)$$

$$L(A_i^{(k+1)}) = k+1-L(A_g^{(k)}) \qquad (7.2.23)$$

$$L(A_i^{(k+1)}) > L(A_i^{(k)}) \qquad (7.2.24)$$

and that $A_i^{(k+1)}$ has minimal length in $E_i^{(k+1)}$ for $0 \leq i < e$. The initialization proving P_0 and the minimality of $A_i^{(0)}$ and $A_i^{(1)}$ is straight forward and details are omitted.

Suppose we are in step k, and case I obtains. Then (7.2.21) holds, and $A_i^{(k+1)}$ has minimal length by induction.

Suppose we have case II(a). We first establish P_k. We may assume (7.2.21) does not hold. Then

$$L(A_i^{(k)}) = 0, \quad A_g^{(k)} = (p^g, 0)$$

and from (7.2.8)

$$S(x)p^g = u_{gk}\, p^{t_{gk}}\, x^k \pmod{x^{k+1}}.$$

This implies that $p^{e-g} = p^{1+t_{ik}}$ divides each of $S_0, S_1, \ldots, S_{k-1}$ and $S_k = u\, p^{t_{gk}-g}$ for some $u \in GR^*(p^e,r)$. Let $S_i = p^{1+t_{ik}}\, S_i^*$ for $i < k$. Using (7.2.8) again and remembering that $a_i^{(k)}(0) = p^i$ we have

$$\left(p^{1+t_{ik}} (S_0^* + S_1^* x + \ldots + S_{k-1}^* x^{k-1}) + u p^{t_{gk}-g} x^k \right).\left(p^i + \ldots\ldots \right)$$

$$= b_i^{(k)}(x) + u_{ik}\, p^{t_{ik}}\, x^k \pmod{x^{k+1}} \qquad (7.2.25)$$

since $L(A_i^{(k+1)}) = k+1 > L(A_i^{(k)})$, and $\deg b_i^{(k)}(x) \leq k-1$. Equating coefficients of x^k in (7.2.23) and using (7.2.9) we obtain

$$sp^{1+t_{ik}} + u\, p^{(t_{gk}+i-e+1+t_{ik})} = u_{ik}\, p^{t_{ik}}$$

for some $s \in GR(p^e,r)$. Since u_{ik} is a unit, it follows that p does not divide $p^{(t_{gk}+i-e+1)}$ i.e., $i+t_{gk} < e$ which is (7.2.22). Next we show that (7.2.23) follows from (7.2.22). In fact we shall show that (7.2.22) implies

$$L(A_i^{(k+1)}) = \max \{ L(A_i^{(k)}),\ k+1-L(A_g^{(k)}) \} \qquad (7.2.26)$$

From (7.2.13), (7.2.15) and (7.2.16) we have

$$L(A_i^{(k+1)}) \leq \max \{ L(A_i^{(k)}),\ k-v+L(A_h^{(v)}) \}$$

$$= \max \{ L(A_i^{(k)}),\ k+1-L(A_g^{(k)}) \}$$

But the reverse inequality follows from Lemma 7.1, using (7.2.17), and establishes (7.2.26). The minimality of $A_i^{(k+1)}$ now follows from (7.2.17), (7.2.18) and Lemma 7.2.

Finally, suppose case IIb obtains. To establish P_k we may assume (7.2.16) does not hold, and so, from (7.2.15) and (7.2.16)

$$k-v+L(A_h^{(v)}) > L(A_i^{(k)})$$

i.e.,
$$k+1 > L(A_i^{(k)})+L(A_g^{(k)}) \qquad (7.2.27)$$

using (7.2.13). Consider the polynomial

$$q(x) = a_i^{(k)}(x)\,[\{ S(x)a_g^{(k)}(x)-b_g^{(k)}(x) \} - a_g^{(k)}(x)\,\{ S(x)a_i^{(k)}(x)-b_i^{(k)}(x) \}]$$

$$= a_g^{(k)}(x)b_i^{(k)}(x) - a_i^{(k)}(x)b_g^{(k)}(x) \qquad (7.2.28)$$

Then just as in (7.2.20) $\deg q(x) \leq L(A_i^{(k)})+L(A_g^{(k)})-1 < k$ by (7.2.27). On the other hand, from (7.2.28)

$$q(x) = (p^{i}+\ldots)(u_{gk}\,p^{t_{ik}}x+\ldots) - (p^{g}+\ldots.)(u_{ik}\,p^{t_{ik}}\,x^{k}+\ldots.) \qquad (7.2.29)$$

containing terms of degree $\geq k$. Therefore $q(x)$ is identically

zero. But the coefficient of x^k in (32) is $u_{gk}\, p^{i+t_{gk}} - u_{ik}\, p^{g+t_{ik}}$ and so

$$i+t_{gk} = g+t_{ik} \qquad (7.2.30)$$

The equation (7.2.24) now follows from (7.2.9). The remainder of the proof is the same as in case IIa.

7.3 A SAMPLE COMPUTATION OF BCH DECODING ALGORITHM

In this Section we display the computation of the algorithm for the BCH code given in Example 6.1, in the form of Table. The BCH code under consideration is a double error correcting code over Z_9 of length 8. We assume that the transmitted codeword is 1 1 6 4 8 8 3 5 and introduce a double error, in fourth and sixth place, i.e., the error vector is 0 0 0 5 0 1 0 0 and hence the received vector is 1 1 6 0 8 0 3 5.

The transform vector of received vector is

$$(60,73,87,46,30,30,12,30).$$

Hence we have the syndromes

$$S_0 = 60, \quad S_1 = 73, \quad S_2 = 87, \quad S_3 = 46, \quad S_4 = 30.$$

i.e., $S(x) = (60) + (73)x + (87)x^2 + (46)x^3 + (30)x^4$

The computation of every step of the algorithm for the above given S(x) is shown in the following pages.

	t=0	t=1
Step 0 k=0	$a_0^{(0)}(x) = (10)$	$a_1^{(0)}(x) = 3(10)$
	$b_0^{(0)}(x) = (00)$	$b_1^{(0)}(x) = (00)$
	$L(A_0^{(0)}) = 0$	$L(A_1^{(0)}) = 0$
	$u_{00} = (20)$	$u_{10} = (10)$
	$t_{00} = 1$	$t_{10} = 2$
	$f(0,0) = 0$	$f(1,0) = 0$
Step 1 k=1	$a_0^{(1)}(x) = (10)$	$a_1^{(1)}(x) = 3(10)$
	$b_0^{(1)}(x) = 3(20)$	$b_1^{(1)}(x) = 3.3(20)=(00)$
	$L(A_0^{(1)}) = 1$	$L(A_1^{(1)}) = 0$
	$u_{01} = (73)$	$u_{11} = (10)$
	$t_{01} = 0$	$t_{11} = 1$
	$g = f(0,1) = 1$	$g = f(1,1) = 0$
		$h = 0$; $r = 0$
Step 2 k=2	$a_0^{(2)}(x) = (10)$	$a_1^{(2)}(x) = (30)+(40)x$
	$b_0^{(2)}(x) = (60)+(73)x$	$b_1^{(2)}(x) = (00)$
	$L(A_0^{(2)}) = 2$	$L(A_1^{(2)}) = 1$
	$u_{02} = (87)$	$u_{12} = (76)$
	$t_{02} = 0$	$t_{12} = 0$
	$g = f(0,2) = 1$	$g = f(1,2) = 1$
	$h = 0$; $r = 1$	$h = 0$; $r = 1$

	t=0	t=1
Step 3 k=3	$a_0^{(3)}(x) = (10)+(72)x$	$a_1^{(3)}(x) = (30)+(36)x$
	$b_0^{(3)}(x) = (60)+(40)x$	$b_1^{(3)}(x) = (30)x$
	$L(A_0^{(3)}) = 2$	$L(A_1^{(3)}) = 2$
	$u_{03} = (53)$	$u_{13} = (20)$
	$t_{03} = 0$	$t_{13} = 1$
	$g = f(0,3) = 1$	$g = f(1,3) = 0$
	$h = 1;\ r = 2$	$h = 1;\ r = 1$
Step 4 k=4	$a_0^{(4)}(x) = (10)+(12)x+(10)x^2$	$a_1^{(4)}(x) = (30)+(36)x+(30)x^2$
	$b_0^{(4)}(x) = (60)+(46)x$	$b_1^{(4)}(x) = (30)x$
	$L(A_0^{(4)}) = 2$	$L(A_1^{(4)}) = 2$
	$u_{04} = (10)$	$u_{14} = (10)$
	$t_{04} = 2$	$t_{14} = 2$

At next step we have

$$a_0^{(5)}(x) = (10)+(12)x+(10)x^2$$

$$b_0^{(5)}(x) = (60)+(46)x \quad \text{and} \quad L(A_0^{(5)}) = 2.$$

Hence we have the connection polynomial to be

$$a(x) = (10)+(12)x+(10)x^2$$

and

$$S(x)a(x) = b(x) \pmod{x^5}.$$

We have

$$S_j = -(a_1 S_{j-1} + a_2 S_{j-2})$$

Putting j=2,3,4,5,6,7 successively we obtain

$S_2 = (87)$; $S_3 = (46)$; $S_4 = (30)$; $S_5 = (26)$; $S_6 = (12)$; $S_7 = (53)$. The inverse transform of $(S_0, S_1, S_2, S_3, S_4, S_5, S_6, S_7)$ gives the error vector to be (0 0 0 5 0 1 0 0). Hence the transmitted codeword is (1 1 6 4 8 8 3 5).

CHAPTER 8

APPLICATIONS

In this chapter we discuss codes over Z_m from the applications point of view.

Codes over Z_m are suitable for channels matched to the Lee metric [29]. All the discrete memoryless symmetric channels matched to the Lee metric have been derived by Chiang and Wolf [29]. Lee metric codes are well suited for phase modulated channels and multilevel quantized pulse amplitude modulated channels [1]. Nemirovskiy [45] has identified some class of multifrequency phase telegraphy signals having the algebraic structure of a ring with an energy advantage.

In this chapter we describe the applications of codes over Z_m in a multichannel communication system and a multiaccess communication system. In Section 8.1, we explain the equivalence of performing a set of DFT in different Galois rings and performing a single DFT in the direct sum of these Galois rings. Transform encoders and decoders for BCH codes over Z_m are described in Section 8.2. The decomposition of a semi-simple ring as a direct sum of Galois fields has been used for efficient coding scheme in a multichannel communication system [31]. The efficiency is in terms of faster computation time in encoding and

decoding. Using the fact that codes over Z_m are direct sum of codes over $Z_{p_i^{k_i}}$, where $m = p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, in Section 8.3, we show that the same advantages in terms of efficiency can be obtained if we use codes over Z_m. In Section 8.4, an efficient coding scheme for a multiaccess communication system, similar to the one discussed in [31], is described. In Section 8.5 we propose to use codes over Z_m as a tool for multiplexing information in a multiaccess communication system using transform encoding and decoding.

8.1 TRANSFORMS ON THE DIRECT SUM OF GALOIS RINGS

Consider the direct sum of Galois rings, $\bigoplus_{i=1}^{t} GR(p_i^{k_i},r)$, denoted by $Q(m,r)$, where $m=p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$. This ring has been discussed in Section 4.2 in connection with spectral characterisation of cyclic codes for $m=p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$. we have

$$Q(m,r) = Z_m[x]/\emptyset(x) \; ; \quad GR(p_i^{k_i},r) = Z_{p_i^{k_i}}[x]/\emptyset_i(x) \quad i=1,2,\ldots,s$$

where $\emptyset_i(x)$ is a monic irreducible polynomial over $Z_{p_i^{k_i}}[x]$ of degree r, i=1,2,...,s, and $\emptyset(x)$, a monic irreducible polynomial of degree r over $Z_m[x]$, is given by

$$\emptyset(x) = (m_1\emptyset_1(x)+m_2\emptyset_2(x)+ \ldots +m_s\emptyset_s(x)) \bmod m$$

where m_i, i=1,2,....s, are chosen such that

$$m_i = 1 \pmod{p_i^{k_i}} \quad ; \quad m_i = 0 \pmod{p_j^{k_j}} \text{ if } i\neq j.$$

We have the isomorphism μ between $Q(m,r)$ and $\bigoplus_{i=1}^{t} GR(p_i^{k_i},r)$ given by

decoding. Using the fact that codes over Z_m are direct sum of codes over $Z_{p_i^{k_i}}$, where $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, in Section 8.3, we show that the same advantages in terms of efficiency can be obtained if we use codes over Z_m. In Section 8.4, an efficient coding scheme for a multiaccess communication system, similar to the one discussed in [31], is described. In Section 8.5 we propose to use codes over Z_m as a tool for multiplexing information in a multiaccess communication system using transform encoding and decoding.

8.1 TRANSFORMS ON THE DIRECT SUM OF GALOIS RINGS

Consider the direct sum of Galois rings, $\bigoplus_{i=1}^{t} GR(p_i^{k_i},r)$, denoted by $Q(m,r)$, where $m=p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$. This ring has been discussed in Section 4.2 in connection with spectral characterisation of cyclic codes for $m=p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$. we have

$$Q(m,r) = Z_m[x]/\emptyset(x) \; ; \quad GR(p_i^{k_i},r) = Z_{p_i^{k_i}}[x]/\emptyset_i(x) \quad i=1,2,\ldots,s$$

where $\emptyset_i(x)$ is a monic irreducible polynomial over $Z_{p_i^{k_i}}[x]$ of degree r, i=1,2,...,s, and $\emptyset(x)$, a monic irreducible polynomial of degree r over $Z_m[x]$, is given by

$$\emptyset(x) = (m_1\emptyset_1(x)+m_2\emptyset_2(x)+ \ldots +m_s\emptyset_s(x)) \bmod m$$

where m_i, i=1,2,....s, are chosen such that

$$m_i = 1 \pmod{p_i^{k_i}} \quad ; \quad m_i = 0 \pmod{p_j^{k_j}} \text{ if } i \neq j.$$

We have the isomorphism μ between $Q(m,r)$ and $\bigoplus_{i=1}^{t} GR(p_i^{k_i},r)$ given by

$$\mu(a) = ((a)_1, (a)_2, \ldots, (a)_s)$$

where $a \in Q(m,r)$ and $(a)_i \in GR(p_i^{k_i},r)$, $i=1,2,\ldots,s$.

If $a = a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1} \in Q(m,r)$

and $(a)_1 = a_{1,0}+a_{1,1}x+a_{1,2}x^2+\ldots.+a_{1,n-1}x^{n-1} \in GR(p_1^{k_1},r)$

$(a)_2 = a_{2,0}+a_{2,1}x+a_{2,2}x^2+\ldots.+a_{2,n-1}x^{n-1} \in GR(p_2^{k_2},r)$

$\vdots \qquad \vdots \qquad \vdots \qquad \vdots$

$(a)_s = a_{s,0}+a_{s,1}x+a_{s,2}x^2+\ldots.+a_{s,n-1}x^{n-1} \in GR(p_s^{k_s},r)$

then under μ, $\mu(a)$ is given by

$$a_{t,0}+a_{t,1}x+\ldots.+a_{t,n-1}x^{n-1} = (a_0+a_1x+a_2x^2+\ldots.+a_{n-1}x^{n-1}) \pmod{p_t^{k_t}}$$

for $t=1,2,\ldots,s$.

The inverse mapping μ^{-1} is given by

$$a_0 = m_1a_{1,0}+m_2a_{2,0}+\ldots.+m_sa_{s,0} \pmod m$$

$$a_1 = m_1a_{1,1}+m_2a_{2,1}+\ldots.+m_sa_{s,1} \pmod m$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$a_{n-1} = m_1a_{1,n-1}+m_2a_{2,n-1}+\ldots.+m_sa_{s,n-1} \pmod m.$$

The isomorphic mapping μ is sometimes called the Chinese remainder theorem transform.

Now suppose $n|(p_i^{k_i},r)$, $i=1,2,\ldots,s$, then a primitive n-th root of unity α_i exists in $GR(p_i^{k_i},r)$, $i=1,2,\ldots,s$. Then $\mu^{-1}(\alpha_1,\alpha_2,\ldots,\alpha_s) = \alpha$ correponds to a primitive n-th root of unity in $Q(m,r)$ and vice versa. Then a length n transform over $GR(p_i^{k_i},r)$, namely

$$A_{t,j} = \sum_{u=0}^{n-1} \alpha_t^{uj} a_{t,u} \; ; \quad j=0,1,\ldots,(n-1) \qquad (8.1.1)$$

for $t=1,2,\ldots,s$, exists. Taking the inverse isomorphic mapping μ^{-1} on the above set of transforms one obtains a length n transform over $Q(m,r)$,

$$A_j = \sum_{u=0}^{n-1} \alpha^{uj} a_u$$

where $A_j=\mu^{-1}(A_{1,j},A_{2,j},\ldots,A_{s,j})$, $a_u=\mu^{-1}(a_{1,u},a_{2,u},\ldots,a_{s,u})$ and $\alpha=\mu^{-1}(\alpha_1,\alpha_2,\ldots,\alpha_s)$ is a primitive n-th root of unity in $Q(m,r)$.

Since $Q(m,r)$ and $\bigoplus_{i=1}^{s} GR(p_i^{k_i},r)$ are isomorphic rings, the set of transforms given by (8.1.1) over $GR(p_i^{k_i},r)$, for $i=1,2,\ldots,s$, can be evaluated using the corresponding transform over $Q(m,r)$. The equivalence of the two systems is shown in Fig 8.1. Assuming that n is a power of two and that FFT algorithm is used to compute the transforms, the system shown in Fig.8.1(a) has a computational complexity of $r(n \log_2 n)$ and the equivalent system shown in Fig.8.1(b) has a computational complexity of $n\log_2 n+2rn$. Thus the system implementing DFT in $Q(m,r)$ is superior to the system implementing DFT is different Galois rings by a factor of $r\log_2 n/(\log_2 n+2r)$ in terms of computational complexity. In the above comparison of the two systems it is assumed that the computational time for multiplications and additions in $GR(p^k,r)$ is the same as the time required for multiplications and additions in $Q(m,r)$. This assumption will roughly hold if a general-purpose computer is used and if the integer m is less than 2^t, where t is a one-word bit length of the computer.

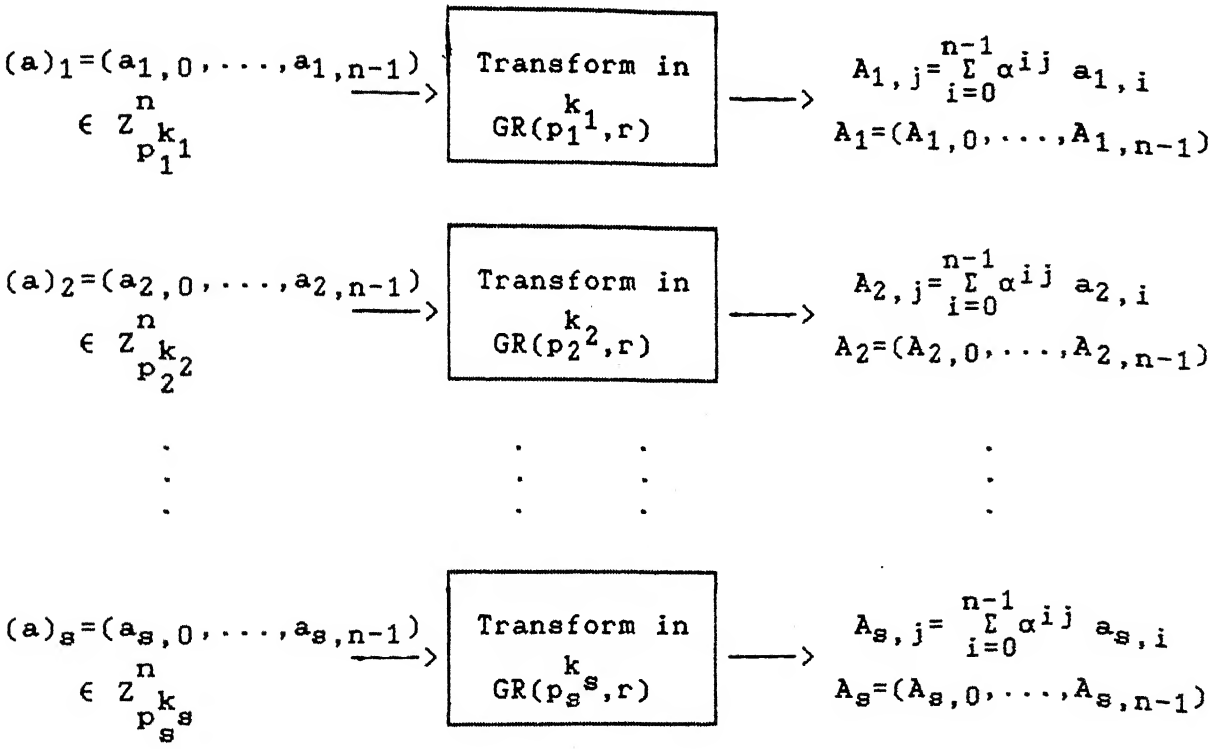


Fig.8.1(a)

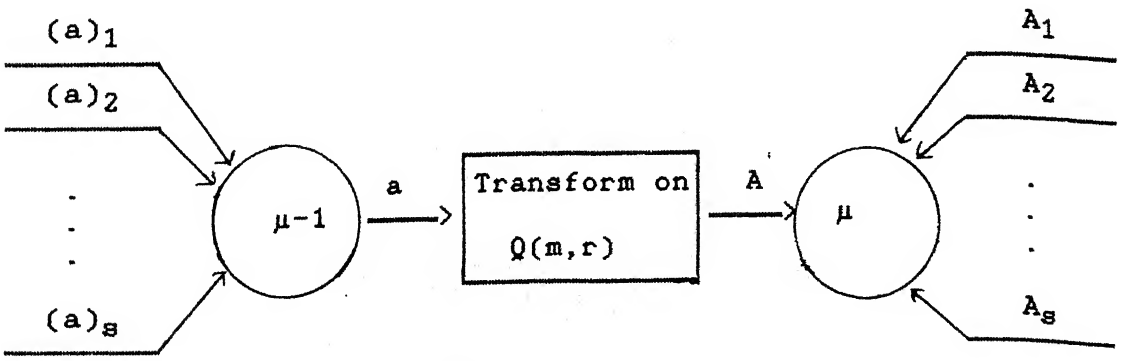


Fig.8.1(b)

Fig.8.1 Equivalence of a set of transforms in $GR(p_i^{k_i},r)$, $i=1,2,\ldots s$, and a transform in $Q(m,r)$.

8.2 TRANFORM ENCODER AND DECODER FOR BCH CODES OVER Z_{p^k}

In this section transform encoder and decoder are described for BCH codes over Z_{p^k} which are defined by d number of consecutive spectral components zeros for all the codewords. For the sake of specificity BCH codes have been assumed, otherwise the description is valid for any cyclic code over Z_{p^k}.

8.2.1 Transform encoder

Let the BCH code over Z_{p^k} under consideration be of length n and let $C_{p,n}(j_1)$, $C_{p,n}(j_2)$, ... $C_{p,n}(j_u)$ be the conjugacy classes with exponents respectively $r_1, r_2, \ldots, r_u$, which take values from the full rings $GR(p^k, r_1)$, $GR(p^k, r_2)$, ... $GR(p^k, r_u)$. Other conjugacy classes take values zeros and the union of these conjugacy classes contain the d consecutive spectral components which define the BCH code. This code is of the form

$$\bigoplus_{i=1}^{u} GR(p^k, r_i)$$

and the word-length μ of this code is given by

$$\mu = r_1(k-0)+r_2(k-0)+\ldots+r_u(k-0) = k(r_1+r_2+\ldots r_u).$$

Hence the number of message symbols is $r_1+r_2+\ldots+r_u = e$, say.

The transform encoder is essentially the implementation of IDFT as shown in Fig 8.2.

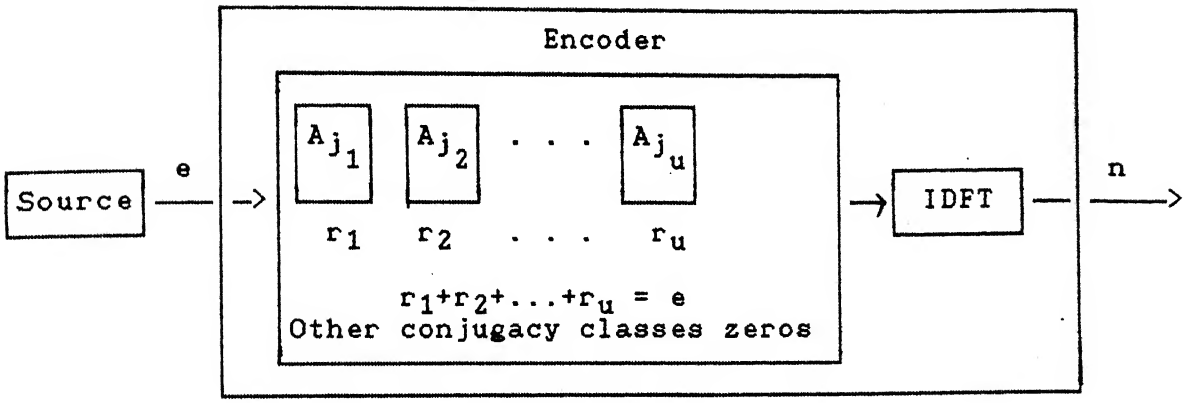
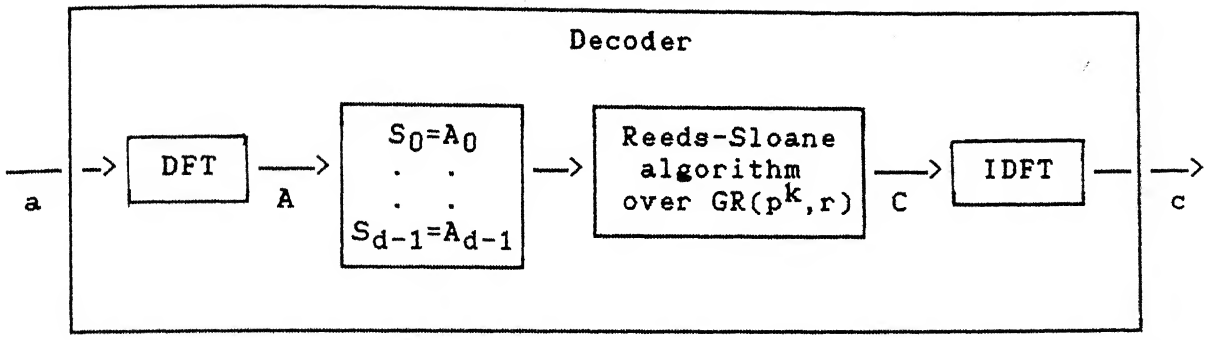


Fig 8.2 Transform encoder

Let $(A_0,A_1,\ldots,A_{n-1})$ be a typical transform vector. The conjugacy class $C_{p,n}(j_i)$, contains the spectral component A_{j_i}, $i=1,2,\ldots,u$. Out of e message symbols r_i, $i=1,2,\ldots,u$, consecutive symbols are assumed to be an element of $GR(p^k,r_i)$ and it is assumed that A_{j_i} is equal to this element of $GR(p^k,r_i)$. The conjugacy symmetry property is used to obtain values of spectral components belonging to the conjugacy class $C_{p,n}(j_i)$, $i=1,2,\ldots,u$. All other conjugacy classes are assigned zeros. Now $(A_0,A_1,\ldots,A_{n-1})$ has been obtained and IDFT of this gives the codeword corresponding to the e message symbols.

8.2.2 Transform decoder

The transform decoder consists of implementations of DFT, Reeds-Sloane algorithm and IDFT as shown in Fig 8.3.



a = received vector $(a_0,a_1,\ldots,a_{n-1})$
A = transform of a = $(A_0,A_1,\ldots,A_{n-1})$
c = transmitted codeword
C = transform of the transmitted codeword
$S_0,S_1,\ldots,S_{d-1}$ are syndromes

Fig 8.3 Transform decoder

Let $a = (a_0,a_1,\ldots,a_{n-1})$ be the received vector. The decoder first obtains the DFT of a, denoted by $A = (A_0,A_1,\ldots,A_{n-1})$. Let us assume that the BCH code under consideration is defined by first d consecutive spectral components equal to zeros. Syndromes $S_0,S_1,\ldots,S_{d-1}$ are obtained by setting the first d components of A equal to respectively $S_0,S_1,\ldots,S_{d-1}$. These syndromes are elements of GR(p^k,r) in which DFT is defined and these are first d spectral components of the unknown error vector. Then using Reeds-Sloane algorithm over GR(p^k,r) discussed in Chapter 7 the transform vector of error vector $(S_0,S_1,\ldots,S_{n-1})$ is obtained. Finally IDFT of $(S_0,S_1,\ldots,S_{n-1})$ gives the error vector, denoted by $(e_0,e_1,\ldots,e_{n-1})$. The transmitted codeword then is given by

$$(c_0,c_1,\ldots,c_{n-1}) = (a_0,a_1,\ldots,a_{n-1})-(e_0,e_1,\ldots,e_{n-1}).$$

In the next section the transform decoder is used in a multichannel communication system which gives computational advantage.

8.3 BCH CODES OVER Z_m FOR MULTICHANNEL COMMUNICATION SYSTEM

In this section application of BCH codes over Z_m to a multichannel communication system is discussed. In a multichannel communication system multiple sources are located in different stations and the coded signals are sent through different channels. All these signals are received and processed at a single station. Fig 8.4 shows a typical multichannel communication system.

The advantage in terms of computation time by using Reed-Solomon codes over finite fields for a multichannel communication system has been discussed in detail in [31]. The main idea used in [31] is that a direct sum of Galois fields is a semi-simple ring. We show that in a multichannel communication system computational advantage can be obtained in the case of BCH codes over Z_m also. In this case the key idea is using the following isomorphism

$$Q(m,r) \equiv GR(p_1^{k_1},r) \oplus GR(p_2^{k_2},r) \oplus \ldots \oplus GR(p_s^{k_s},r). \quad (8.2)$$

given by the mapping μ,

$$\mu(r(x)) = (r_1(x), r_2(x), \ldots, r_s(x))$$

where $r(x) \in Q(m,r)$ and $r_i(x) \in GR(p_i^{k_i},r)$, $i=1,2,\ldots,s$.

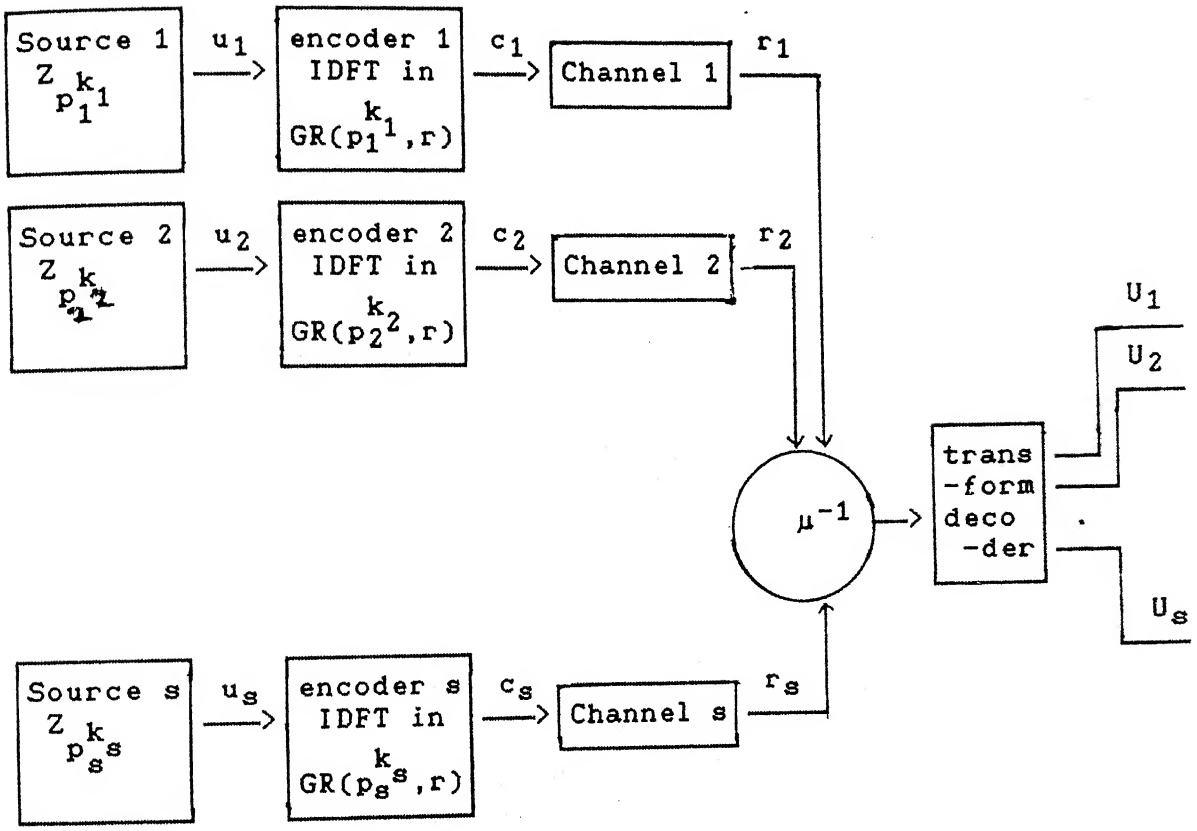


Fig.8.4 Multichannel communication system using transform encoder and decoder.

Let us consider a multichannel communication system with s sources as shown in Fig 8.4. It is assumed that, for j=1,2,...,s, symbols from Source j are from $Z_{p_j^{k_j}}$. A BCH code over $Z_{p_j^{k_j}}$ is used for Source j. Source vectors u_j, j=1,2,...,s, are encoded into BCH codewords $c_j(x)$ using transform encoding. These codewords are sent over the channels and $r_j(x)$ is the received vector at the j-th receiver.

At the receiver, system shown in Fig.8.1(b) is used to compute the transforms of the received vectors $r_k(x)$, k=1,2,...s. First the inverse mapping μ-1 is applied to obtain the corresponding vector $r(x) \in Z_m^n$. Then a DFT defined over Q(m,r) is used to obtain syndromes $S_j(\alpha^j)$ for j=1,2,...,2t. Again the decomposition of these syndromes using the isomorphism μ gives syndromes for individual sources. Then using the principle of transform decoder discussed in the previous section for individual syndrome sequences, error vectors for each source are obtained.

The efficiency in this system is due to the fact that a set of transforms to be computed in Galois rings $GR(p_i^{k_i},r_i)$ is computed by a single transform in Q(m,r) which is the direct sum of Galois rings. The efficiency in terms computational advantage in computing DFT in Q(m,r) has been already discussed in Section 8.1.

8.4 CODES OVER Z_m AS A TOOL FOR MULTIPLEXING IN MULTI-ACCESS COMMUNICATION SYSTEM

In a multi-access communication system different sources are located at one station and a single encoder is used to encode messages from all the sources. Fig 8.5 shows a typical multi-access communication system. The primary difference between this system and the multichannel communication system discussed in the previous section is that the encoded signals are sent through one wide band channel instead of separate channels.

Now we consider the multiple access communication system shown in Fig 8.5. In this system the different sources are encoded using the transform on finite ring Q(m,r). Symbols from source i are from $Z_{p_i^{k_i}}$, i=1,2,...,s. The vector u_i is the information symbol vector from source i. The isomorphism μ is used to obtain $u \in Z_m[x]$ for a given sequence $u_1, u_2, \ldots, u_s$ from different sources. u is used to fill conjugacy classes in DFT over Q(m,r). Then inverse DFT in Q(m,r) gives codeword c of a code over Z_m. Let r be the received vector. DFT of r gives syndromes in Q(m,r). Then using isomorphism μ syndromes for individual sources are obtained. Then for BCH codes using the transform decoder discussed in Section 8.2 error vector for all the sources can be obtained.

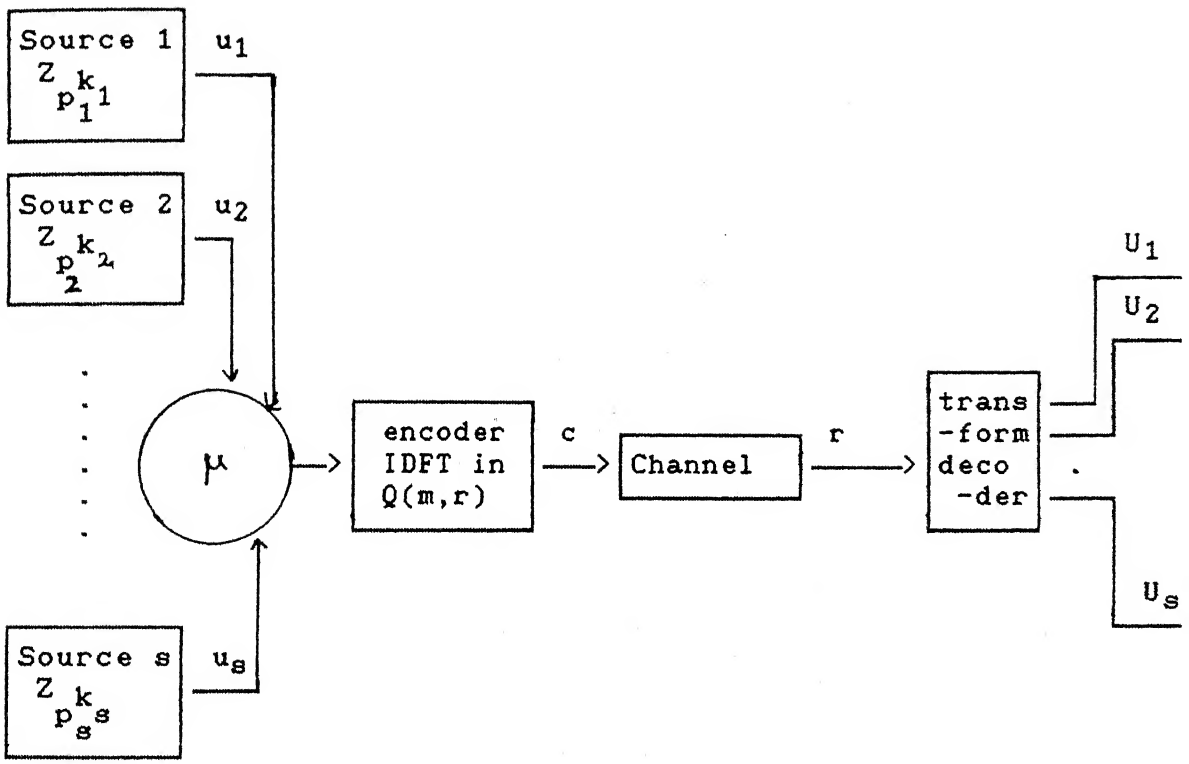


Fig.8.5 Multiplexing in a multiaccess communication system: Size of the alphabet of different sources are powers of different primes.

In the system discussed in Section 8.1 each source had a separate channel and a codeword over $Z_{p_i^{k_i}}$, whereas in the system shown in Fig 8.3, sources do not have individual codewords over $Z_{p_i^{k_i}}$. One codeword of a code over Z_m is used to transmit through the channel, corresponding to a set of information sequences from all sources. So essentially a code over Z_m has been used and the achievement of multiplexing is clear.

In the system of Fig.8.5 multiplexing has been achieved due to the fact that a code over Z_m is a direct sum of codes over $Z_{p_i^{k_i}}$. Moreover it is seen that each source is associated with different primes. We can achieve multiplexing even when different sources give symbols from Z_{p^k}. We assume that symbols from source i are from the ideal $p^{j_i}Z_{p^k}$, $j_i=0,1,\ldots,k$, $i=1,2,\ldots,s$. Fig 8.6 shows the communication system for this case. The key idea in this case is using Inverse DFT over $GR(p^k,r)$ for encoding using different conjugacy classes for symbols from different sources, and using the direct sum structure given by the isomorphism of Theorem 4.1, i.e.,

$$R_T \equiv Z_{p^k}[x]/(x^n-1) \equiv \bigoplus_{i=1}^{t} GR(p^k,r_i)$$

Let us assume that a BCH code is used. Leaving the conjugacy classes which take zero values, each of the remaining conjugacy classes are filled with symbols from each source. Let symbols from source i are used to fill the conjugacy class $C_{p,n}(t_i)$, such that $C_{p,n}(t_i)$, $i=1,2,\ldots,s$ are disjoint. Then IDFT in $GR(p^k,r)$ used as encoder obtains a codeword c and let r be the received

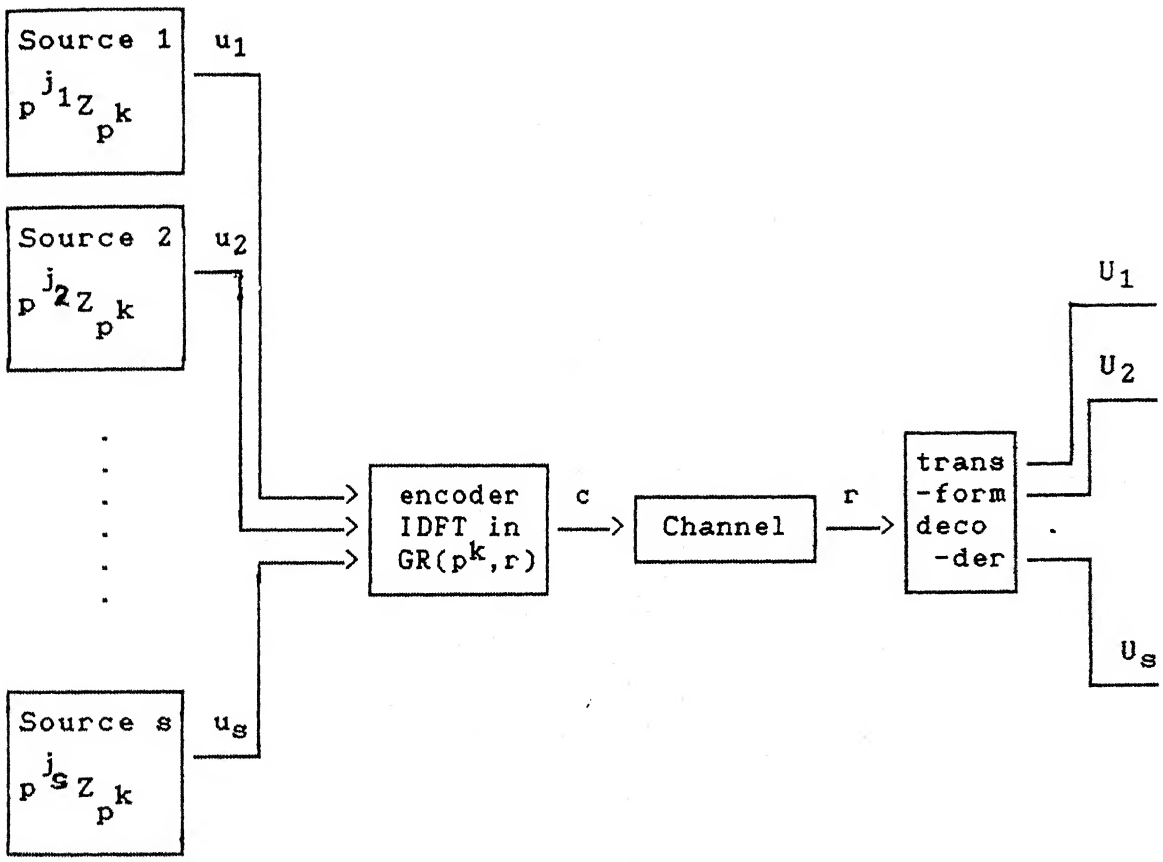


Fig.8.6 Multiplexing in a multiaccess communication system. Size of the alphabet of different sources are powers of same prime.

vector. BCH decoding algorithm of Chapter 6 is used to obtain c and DFT of c gives the transmitted symbols of all sources in respective conjugacy classes.

The advantages of this system is that single transform in $GR(p^k,r)$, is sufficient for the decoding and encoding for several sources. However the choice of n will face the following constraints. The number of conjugacy classes, t should be at least equal to the number of sources and number of conjugacy classes for zeros. Also the exponents of the conjugacy classes used for information symbols should match with the length of information sequences U_i, i=1,2,...,s. i.e., length of U_i should be r_i.

CHAPTER 9

CONCLUSION

In this chapter, the concluding chapter of this thesis, we give a summary of the results obtained in this thesis and give few suggestions regarding possible further research along the lines of approach of this thesis.

9.1 SUMMARY OF THE RESULTS

The results obtained in this thesis may be summarised as follows:

Linear codes over Z_m are defined as submodules of the module of the set of n-tuples over Z_m. Zero divisors of Z_m, which give rise to non-trivial ideals, present situations the counterparts of which are missing in the case of linear codes over finite fields. It is seen that some linear codes cannot be used for source with alphabet size m. It is proposed that these codes can be used for coding simultaneously more than one source. This requires the introduction of notion of word-length of a linear code over Z_m, which is the courterpart of dimension of a linear code over finite field.

The class of cyclic codes and its generalisation, Abelian codes over Z_m, are studied in the transform domain. Given Z_m and length of the code n, our starting point is the identification of appropriate extension ring of Z_m, which supports a DFT of length n. This requires the condition that the code length n should be relatively prime to m, which is assumed throughout the thesis.

For $m=p^k$, the appropriate extension ring is the Galois ring $GR(p^k,r)$ where r is the least integer such that code length n divides (p^r-1). The discrete Fourier transform (DFT) defined in this Galois ring establishes an isomorphism between convolution algebra of n-tuples over Z_{p^k} and pointwise product algebra of n-tuples over $GR(p^k,r)$. In a transform vector the DFT coefficients of a conjugacy class are related by the generator of the automorphism group of $GR(p^k,r)$. It is shown that the image of the set of n-tuples over Z_{p^k} as a ring with cyclic convolution as multiplication is isomorphic to a direct sum of subrings of $GR(p^k,r)$. Using this isomorphism it is shown that a cyclic code over Z_{p^k} consists of those n-tuples over Z_{p^k} whose transform vectors have elements of particular ideal of the extension ring, including nontrivial ideals, in the specified conjugacy classes. The cyclic codes which take zeros in the transform domain in all the conjugacy classes except in one are defined as minimal and submininal cyclic codes; if the single conjugacy class takes full ring it is called minimal cyclic code and if it takes a non-trivial ideal it is called sub-minimal cyclic code. From these definitions it follows that any cyclic code over Z_{p^k} is a direct

sum of minimal and subminimal cyclic codes. Regarding Hamming distance of the cyclic codes it is proved that cyclic codes which are defined by elements from non-trivial ideals in a set of conjugacy classes have the same Hamming distance as the cyclic codes which are defined by elements from the full ring in the same set of conjugacy classes, the ideals in all other conjugacy classes being zero ideal. Regarding Lee distance of the cyclic codes some specific codes have been pointed out where, for the same number of codewords, cyclic codes with non-trivial ideals in some conjugacy classes have greater Lee distance than cyclic codes with only trivial ideals in all the conjugacy classes.

For arbitrary values of $m = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, it is shown that the appropriate extension ring which supports a DFT is a direct sum of Galois rings. Proceeding in similar lines as for the case of $m=p^k$, it is observed that every cyclic code over Z_m is a direct sum of cyclic codes over $Z_{p_i^{k_i}}$, $i=1,2,\ldots,s$.

For the special case of m being a product of distinct primes, since $Z_m[x]/(x^n-1)$ is a semi-simple ring every cyclic code over Z_m has an idempotent generator. It is shown that there is a simple way of identifying the idempotent generators in the transform domain using only the idempotent elements of Z_m.

Then we extend this transform approach of cyclic codes over Z_m to Abelian codes over Z_m. The key idea that enables this generalisation is shown to be changing the indexing scheme for

codeword components and DFT coefficients. In the case of cyclic codes indexing scheme is { 0,1,...,n-1 }, elements of a fixed radix number system. It is proved that for Abelian codes, with appropriately chosen mixed-radix number system for indexing depending upon the factorization of the Abelian group in to a direct product of its cyclic subgroups, a Generalised DFT (GDFT) can be defined which maps the generalised convolution operation determined by the Abelian group on the set of n-tuples over Z_m, to pointwise multiplication in the set of n-tuples over the extension ring. The counterpart of conjugacy classes for DFT is shown to be the conjugacy classes defined in the mixed-radix number system for the GDFT. With this GDFT and conjugacy classes in mixed-radix number systems, results similar to those obtained for cyclic codes are obtained for Abelian codes. These include spectral characterisation, results concerning Hamming distance and identifying in a simple way all the idempotent generators in the semi-simple case.

Dual code of linear codes over Z_m is defined along the lines of Delsarte's definition of dual code of an additive code, which reduces to the classical definition of orthogonal complement for linear codes over finite fields. For both cyclic and Abelian codes, dual code pairs are characterised in terms of spectral components of codewords as follows. If L is a cyclic or abelian code over Z_{p^k} whose transform vectors take values from the ideals $I_1, I_2, \ldots, I_t$ for the conjugacy classes $C_{p,n}(j_1)$, $C_{p,n}(j_2), \ldots C_{p,n}(j_t)$ respectively then the transform vectors of

the dual code of L take values from the ideals $(I_1)_d,(I_2)_d,\ldots,(I_t)_d$ respectively for the conjugacy classes $C_{p,n}(n-j_1)$, $C_{p,n}(n-j_2),\ldots,C_{p,n}(n-j_t)$. The non-existence result that states " When n and m are relatively prime and $m=p_1^{k_1}p_2^{k_2}\ldots p_s^{k_s}$, self-dual cyclic codes and self-dual Abelian codes do not exist if any one of k_i, i=1,2,...,s, is an odd integer." is proved.

A decoding algorithm is obtained for BCH codes over Z_{p^k} which is defined in the transform domain by consecutive spectral components being equal to zero. It is shown that the problem of decoding these codes is equivalent to the problem of synthesizing a minimal shift register sequence over a Galois ring. An algorithm for minimal shift register synthesis over Galois ring is obtained by incorporating a minor modification in the already known shift register systhesis algorithm for sequences over Z_{p^k}, obtained by Reeds and Sloane.

Finally, it is shown that codes over Z_m can be used in computationally efficient implementation of multi-channel communication system. The computational efficiency is due to the fact that a set of transforms over several Galois rings can be achieved by a single transform over a direct sum of these Galois rings. The equivalence of transforms over several Galois rings and a transform over their direct sum is explained in detail. It is also proposed to use codes over Z_m as a tool for multiplexing

information in multi-user communication systems. The following two different situations are considered for miltiplexing. (i) The size of the alphabets of different sources are powers of different primes and (ii) The size of the alphabets of different sources are different powers of a prime.

9.2 SUGGESTIONS FOR FURTHER RESEARCH

In this section few directions are suggested along which further investigation of codes over Z_m can be carried out.

(1) We have discussed codes over Z_m which includes codes over GF(p) as a special case. It will be of interest to investigate codes over a Galois ring. Since Galois rings include as particular cases GF(p), $GF(p^k)$ and Z_{p^k}, it will provide a general theory that will include codes over finite fields, both prime fields and non-prime fields, and codes over Z_m. Such an attempt will not face much difficulty since the approach is similar to the approach we have taken for codes over Z_m. It is more or less the question of working out details for automorphisms of a Galois ring which leaves invariant a subring, not Z_{p^k}, of it.

(2) Codes over Galois rings seems to be important for developing a theory for codes over any arbitrary finite comutative ring

with identity. Our belief is based on the following results already available.

(i) Any finite commutative ring with identity can be decomposed as a direct sum of local rings [13].

(ii) Any finite commutative local ring with identity is isomorphic to a homomorphic image of a polynomial ring over a Galois ring [13, Theorem XVII].

(iii) The most general algebraic structure needed to implement DFT on finite rings is a direct sum of Galois rings [30].

(3) In this thesis we have developed decoding algorithm for BCH codes over Z_m which are defined by consecutive DFT components being zeros. Our decoding algorithm is for Hamming metric. Since codes over Z_m are suitable for Lee metric channels it will be of interest to investigate algorithms for decoding for the Lee metric.

(4) We have extended the transform approach for cyclic codes to Abelian codes. The problem essentially was to develop a transform which maps the generalised convolution defined by the Abelian group to pointwise multiplication. Codewords of a cyclic code can be considered as functions defined over an index set $I = \{ 0,1,\ldots,n-1 \}$ which is assumed to have

codewords of an Abelian group can be considered to be functions defined over an index set which has the structure of an Abelian group. Our suggestion is to impose the structure of monoid, to start with cyclic monoid, on the index set and try to develop a suitable transform for it, which may result in 'monoid codes'.

(5) Comparing the results available for block codes over finite fields, to our knowledge, very few results are available in the literature for block codes over Z_m. It will be of considerable interest to investigate which are the notions existing for finite fields can be extended or similar notion can be defined for Z_m. Such an investigation may give interesting results which are counterparts of results for codes over finite fields.

APPENDIX A

LISTING OF ALL CYCLIC CODES OF LENGTH 3 OVER Z8 WITH SPECTRUM

The extension ring for length 3 cyclic codes over Z_8 is GR(8,2). An element a+bx of GR(8,2) is represented simply by ab. The conjugacy classes are $C_{2,3}(0) = \{0\}$ and $C_{2,3}(1) = \{1,2\}$. Cyclic codes are ideals of

$$Z_8[x]/(x3-1) \equiv GR(8,1) \oplus GR(8,2)$$

The conjugacy class {0} takes values from an ideal of GR(8,1) and the conjugacy class {1,2} takes values from an ideal of GR(8,2). Ideals of GR(8,1) are zero ideal, 2GR(8,1), 2^2GR(8,1) and GR(8,1) and Ideals of GR(8,2) are zero ideal, 2GR(8,2), 2^2GR(8,2) and GR(8,2). All the codewords of all the codes with their spectrum are listed below.

Code N1:

codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	4 4 4	40 00 00

Code N2

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	4 4 0	00 44 04	4 0 4	00 04 44
0 4 4	00 40 40				

Code N3:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	2 2 2	60 00 00	4 4 4	40 00 00
6 6 6	20 00 00				

Code N4:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	4 0 0	40 40 40	4 0 4	00 04 44
0 4 0	40 04 44	0 4 4	00 40 40	4 4 0	00 44 04
0 0 4	40 44 04	4 4 4	40 00 00		

Code N5:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	1 1 1	30 00 00	2 2 2	60 00 00
3 3 3	10 00 00	4 4 4	40 00 00	5 5 5	70 00 00
6 6 6	20 00 00	7 7 7	40 00 00		

Code N6:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	6 2 0	00 62 46	4 2 2	00 20 20
2 2 4	00 66 02	0 2 6	00 24 64	4 4 0	00 44 04
2 4 2	00 02 66	0 4 4	00 40 40	6 4 6	00 06 22
2 6 0	00 26 42	0 6 2	00 64 24	6 6 4	00 22 06
4 6 6	00 60 60	6 0 2	00 46 62	4 0 4	00 04 44
2 0 6	00 42 26				

Code N7:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	4 0 0	40 40 40	6 2 2	20 40 40
4 0 4	00 04 44	6 2 6	60 04 44	0 4 0	40 04 44
2 6 2	20 04 44	0 4 4	00 40 40	2 6 6	60 40 40
4 4 0	00 44 04	6 6 2	60 44 04	4 4 4	40 00 00
6 6 6	20 00 00	2 2 2	60 00 00	0 0 4	40 44 04
2 2 6	20 44 04				

Code N8:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	4 0 0	40 40 40	4 4 0	00 44 04
6 0 2	00 46 62	6 4 2	40 42 26	4 0 4	00 04 44
4 4 4	40 00 00	6 0 6	40 02 66	6 4 6	00 06 22
2 2 0	40 22 06	2 6 0	00 26 42	0 2 2	40 60 60
0 6 2	00 64 24	2 2 4	00 66 02	2 6 4	40 62 46

(continued..)

0 2 6	00 24 64	0 6 6	40 20 20	6 2 0	00 62 46
6 6 0	40 66 02	4 2 2	00 20 20	4 6 2	40 24 64
6 2 4	40 26 42	6 6 4	00 22 06	4 2 6	40 64 24
4 6 6	00 60 60	0 4 0	40 04 44	2 0 2	40 06 22
2 4 2	00 02 66	0 0 4	40 44 04	0 4 4	00 40 40
2 0 6	00 42 26	2 4 6	40 46 62		

Code N9:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	4 0 0	40 40 40	5 1 1	70 40 40
6 2 2	20 40 40	7 3 3	50 40 40	4 0 4	00 04 44
5 1 5	30 04 44	6 2 6	60 04 44	7 3 7	10 04 44
0 4 0	40 04 44	1 5 1	70 04 44	2 6 2	20 04 44
3 7 3	50 04 44	0 4 4	00 40 40	1 5 5	30 40 40
2 6 6	60 40 40	3 7 7	10 40 40	4 4 0	00 44 04
5 5 1	30 44 04	6 6 2	60 44 04	7 7 3	10 44 04
4 4 4	40 00 00	5 5 5	70 00 00	6 6 6	20 00 00
7 7 7	50 00 00	1 1 1	30 00 00	2 2 2	60 00 00
3 3 3	10 00 00	0 0 4	40 44 04	1 1 5	70 44 04
2 2 6	20 44 04	3 3 7	50 44 04		

Code N10:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	0 4 2	60 62 46	2 0 0	20 20 20
0 6 2	00 64 24	2 2 0	40 22 06	0 0 4	40 44 04
2 4 0	60 24 64	0 2 4	60 46 62	2 6 0	00 26 42
0 4 4	00 40 40	2 0 2	40 06 22	0 6 4	20 42 26
2 2 2	60 00 00	0 0 6	60 22 06	2 4 2	00 02 66
0 2 6	00 24 64	2 6 2	20 04 44	0 4 6	20 26 42
2 0 4	60 64 24	0 6 6	40 20 20	2 2 4	00 66 02
0 2 2	40 60 60	2 4 4	20 60 60	2 6 4	40 62 46
2 0 6	00 42 26	2 2 6	20 44 04	2 4 6	40 46 62
2 6 6	60 40 40	4 0 0	40 40 40	4 2 0	60 42 26
4 4 0	00 44 04	4 6 0	20 46 62	4 0 2	60 26 42
4 2 2	00 20 20	4 4 2	20 22 06	4 6 2	40 24 64
4 0 4	00 04 44	4 2 4	20 06 22	4 4 4	40 00 00
4 6 4	60 02 66	4 0 6	20 62 46	4 2 6	40 64 24
4 4 6	60 66 02	4 6 6	00 60 60	6 0 0	60 60 60
6 2 0	00 62 46	6 4 0	20 64 24	6 6 0	40 66 02
6 0 2	00 46 62	6 2 2	20 40 40	6 4 2	40 42 26
6 6 2	60 44 04	6 0 4	20 24 64	6 2 4	40 26 42
6 4 4	60 20 20	6 6 4	00 22 06	6 0 6	40 02 66
6 2 6	60 04 44	6 4 6	00 06 22	6 6 6	20 00 00
0 2 0	20 02 66	0 4 0	40 04 44	0 6 0	60 06 22
0 0 2	20 66 02				

Code N11:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	5 0 3	00 25 53	7 1 0	00 71 67
1 4 3	00 61 57	3 5 0	00 35 63	4 0 4	00 04 44
6 1 1	00 50 50	0 4 4	00 40 40	2 5 1	00 14 54
3 0 5	00 63 35	5 1 2	00 37 41	7 4 5	00 27 31
1 5 2	00 73 45	2 0 6	00 42 26	4 1 3	00 16 32
6 4 6	00 06 22	0 5 3	00 52 36	1 0 7	00 21 17
3 1 4	00 75 23	5 4 7	00 65 13	7 5 4	00 31 27
2 1 5	00 54 14	5 7 4	00 13 65	6 5 5	00 10 10
1 1 6	00 33 05	5 5 6	00 77 01	0 1 7	00 12 76
4 5 7	00 56 72	6 2 0	00 62 46	2 6 0	00 26 42
5 2 1	00 41 37	1 6 1	00 05 33	4 2 2	00 20 20
0 6 2	00 64 24	3 2 3	00 07 11	7 6 3	00 43 15
2 2 4	00 66 02	6 6 4	00 22 06	1 2 5	00 45 73
5 6 5	00 01 77	0 2 6	00 24 64	4 6 6	00 60 60
7 2 7	00 03 55	3 6 7	00 47 51	5 3 0	00 53 25
1 7 0	00 17 21	4 3 1	00 32 16	0 7 1	00 76 12
3 3 2	00 11 07	7 7 2	00 55 03	2 3 3	00 70 70
6 7 3	00 34 74	1 3 4	00 57 61	0 3 5	00 36 52
4 7 5	00 72 56	7 3 6	00 15 43	3 7 6	00 51 47
6 3 7	00 74 34	2 7 7	00 30 30	4 4 0	00 44 04
7 0 1	00 67 71	3 4 1	00 23 75	6 0 2	00 46 62
2 4 2	00 02 66				

Code N12:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	2 5 5	40 50 50	1 4 3	00 61 57
4 0 0	40 40 40	0 7 5	40 32 16	3 6 3	40 03 55
6 2 0	00 62 46	1 1 6	00 33 05	0 0 4	40 44 04
4 4 0	00 44 04	3 3 6	40 55 03	2 2 4	00 66 02
6 6 0	40 66 02	1 5 6	40 37 41	0 4 4	00 40 40
7 0 1	00 67 71	3 7 6	00 51 47	2 6 4	40 62 46
5 2 1	00 41 37	0 1 7	00 12 76	3 0 5	00 63 35
7 4 1	40 63 35	2 3 7	40 34 74	1 2 5	00 45 73
5 6 1	40 45 73	0 5 7	40 16 32	3 4 5	40 67 71
6 0 2	00 46 62	2 7 7	00 30 30	1 6 5	40 41 37
4 2 2	00 20 20	7 1 0	00 71 67	2 0 6	00 42 36
6 4 2	40 42 26	5 3 0	00 53 25	0 2 6	00 24 64
4 6 2	40 24 64	7 5 0	40 75 23	2 4 6	40 46 62
5 0 3	00 25 53	5 7 0	40 57 61	0 6 6	40 20 20
7 2 3	40 47 51	6 1 1	00 50 50	1 0 7	00 21 17
5 4 3	40 21 17	4 3 1	00 32 16	3 2 7	40 43 15
7 6 3	00 43 15	6 5 1	40 54 14	1 4 7	40 25 53
4 0 4	00 04 44	4 7 1	40 36 52	3 6 7	00 47 51
6 2 4	40 26 42	5 1 2	00 37 41	2 1 5	00 54 14

(continued..)

4 4 4	40 00 00	7 3 2	40 51 47	1 0 3	40 65 13
6 6 4	00 22 06	5 5 2	40 33 05	0 3 5	00 36 52
7 0 5	40 23 75	7 7 2	00 55 03	3 2 3	00 07 11
5 2 5	40 05 33	4 1 3	00 16 32	7 4 5	00 27 31
6 3 3	40 30 30	5 6 5	00 01 77	4 5 3	40 12 76
6 0 6	40 02 66	6 7 3	00 34 74	4 2 6	40 64 24
7 1 4	40 35 63	6 4 6	00 06 22	5 3 4	40 17 21
4 6 6	00 60 60	7 5 4	00 31 27	5 0 7	40 61 57
5 7 4	00 13 65	7 2 7	00 03 55	6 1 5	40 14 54
5 4 7	00 65 13	4 3 5	40 76 12	7 6 7	40 07 11
6 5 5	00 10 10	3 1 0	40 31 27	4 7 5	00 72 56
1 3 0	40 13 65	5 1 6	40 73 45	3 5 0	00 35 63
7 3 6	00 15 43	1 7 0	00 17 21	5 5 6	00 77 01
2 1 1	40 10 10	7 7 6	40 11 07	0 3 1	40 72 56
4 1 7	40 52 36	2 5 1	00 14 54	6 3 7	00 74 34
0 7 1	00 76 12	4 5 7	00 56 72	1 1 2	40 77 01
6 7 7	40 70 70	3 3 2	00 11 07	2 2 0	40 22 06
1 5 2	00 73 45	0 4 0	40 04 44	3 7 2	40 15 43
2 6 0	00 26 42	0 1 3	40 56 72	3 0 1	40 27 31
2 3 3	00 70 70	1 2 1	40 01 77	0 5 3	00 52 36
3 4 1	00 23 75	2 7 3	40 74 34	1 6 1	00 05 33
3 1 4	00 75 23	2 0 2	40 06 22	1 3 4	00 57 61
0 2 2	40 60 60	3 5 4	40 71 67	2 4 2	00 02 66
1 7 4	40 53 25	0 6 2	00 64 24		

Code N13:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	5 5 5	70 00 00	1 5 3	10 62 46
2 0 0	20 20 20	5 7 5	10 02 66	1 7 3	30 64 24
2 2 0	40 22 06	4 0 6	20 62 46	0 0 4	40 44 04
2 4 0	60 24 64	4 2 6	40 64 24	0 2 4	60 46 62
2 6 0	00 26 42	4 4 6	60 66 02	0 4 4	00 40 40
3 1 1	50 20 20	4 6 6	00 60 60	0 6 4	20 42 26
3 3 1	70 22 06	5 1 7	50 62 46	1 1 5	70 44 04
3 5 1	10 24 64	5 3 7	70 64 24	1 3 5	10 46 62
3 7 1	30 26 42	5 5 7	10 66 02	1 5 5	30 40 40
2 0 2	40 06 22	5 7 7	30 60 60	1 7 5	50 42 26
2 2 2	60 00 00	6 0 0	60 60 60	0 0 6	60 22 06
2 4 2	00 02 66	6 2 0	00 62 46	0 2 6	00 24 64
2 6 2	20 04 44	6 4 0	20 64 24	0 4 6	20 26 42
3 1 3	70 06 22	6 6 0	40 66 02	0 6 6	40 20 20
3 3 3	10 00 00	7 1 1	10 60 60	1 1 7	10 22 06
3 5 3	30 02 66	7 3 1	30 62 46	1 3 7	30 24 64
3 7 3	50 04 44	7 5 1	50 64 24	1 5 7	50 26 42
2 0 4	60 64 24	7 7 1	70 66 02	1 7 7	70 20 20
2 2 4	00 66 02	6 0 2	00 46 62	5 1 5	30 04 44
2 4 4	20 60 60	6 2 2	20 40 40	1 1 3	50 66 02
2 6 4	40 62 46	6 4 2	40 42 26	5 3 5	50 06 22

(continued..)

3 1 5	10 64 24	6 6 2	60 44 04	1 3 3	70 60 60
3 3 5	30 66 02	7 1 3	30 46 62	3 5 5	50 60 60
7 3 3	50 40 40	3 7 5	70 62 46	7 5 3	70 42 26
2 0 6	00 42 26	7 7 3	10 44 04	2 2 6	20 44 04
6 0 4	20 24 64	2 4 6	40 46 62	6 2 4	40 26 42
2 6 6	60 40 40	6 4 4	60 20 20	3 1 7	30 42 26
6 6 4	00 22 06	3 3 7	50 44 04	7 1 5	50 24 64
3 5 7	70 46 62	7 3 5	70 26 42	3 7 7	10 40 40
7 5 5	10 20 20	4 0 0	40 40 40	7 7 5	30 22 06
4 2 0	60 42 26	6 0 6	40 02 66	4 4 0	00 44 04
6 2 6	60 04 44	4 6 0	20 46 62	6 4 6	00 06 22
5 1 1	70 40 40	6 6 6	20 00 00	5 3 1	10 42 26
7 1 7	70 02 66	5 5 1	30 44 04	7 3 7	10 04 44
5 7 1	50 46 62	7 5 7	30 06 22	4 0 2	60 26 42
7 7 7	50 00 00	4 2 2	00 20 20	0 2 0	20 02 66
4 4 2	20 22 06	0 4 0	40 04 44	4 6 2	40 24 64
0 6 0	60 06 22	5 1 3	10 26 42	1 1 1	30 00 00
5 3 3	30 20 20	1 3 1	50 02 66	5 5 3	50 22 06
1 5 1	70 04 44	5 7 3	70 24 64	1 7 1	10 06 22
4 0 4	00 04 44	0 0 2	10 66 02	4 2 4	20 06 22
0 2 2	40 60 60	4 4 4	40 00 00	0 4 2	60 62 46
4 6 4	60 02 66	0 6 2	00 64 24		

Code N14:

codeword	spectrum	codeword	spectrum	codeword	spectrum
0 0 0	00 00 00	2 6 6	60 40 40	4 5 5	60 70 70
2 0 0	20 20 20	3 7 6	00 51 47	5 6 5	00 01 77
3 1 0	40 31 27	3 0 7	20 41 37	4 7 5	00 72 56
2 2 0	40 22 06	2 1 7	20 32 16	4 0 6	20 62 46
3 3 0	60 33 05	3 2 7	40 43 15	5 1 6	40 73 45
2 4 0	60 24 64	2 3 7	40 34 74	4 2 6	40 64 24
3 5 0	00 35 63	3 4 7	60 45 73	5 3 6	60 75 23
2 6 0	00 26 42	2 5 7	60 36 52	4 4 6	60 66 02
3 7 0	20 37 41	3 6 7	00 47 51	5 5 6	00 77 01
3 0 1	40 27 31	2 7 7	00 30 30	4 6 6	00 60 60
2 1 1	40 10 10	4 0 0	40 40 40	5 7 6	20 71 67
3 2 1	60 21 17	5 1 0	60 51 47	5 0 7	40 61 57
2 3 1	60 12 76	4 2 0	60 42 26	4 1 7	40 52 36
3 4 1	00 23 75	5 3 0	00 53 25	5 2 7	60 63 35
2 5 1	00 14 54	4 4 0	00 44 04	4 3 7	60 54 14
3 6 1	20 25 53	5 5 0	20 55 03	5 4 7	00 65 13
2 7 1	20 16 32	4 6 0	20 46 62	4 5 7	00 56 72
2 0 2	40 06 22	5 7 0	40 57 61	5 6 7	20 67 71
3 1 2	60 17 21	5 0 1	60 47 51	4 7 7	20 50 50
2 2 2	60 00 00	4 1 1	60 30 30	6 0 0	60 60 60
3 3 2	00 11 07	5 2 1	00 41 37	7 1 0	00 71 67
2 4 2	00 02 66	4 3 1	00 32 16	6 2 0	00 62 46

(continued..)

3	5	2	20	13	65	5	4	1	20	43	15	7	3	0	20	73	45
2	6	2	20	04	44	4	5	1	20	34	74	6	4	0	20	64	24
3	7	2	40	15	43	5	6	1	40	45	73	7	5	0	40	75	23
3	0	3	60	05	33	4	7	1	40	36	52	6	6	0	40	66	02
2	1	3	60	76	12	4	0	2	60	26	42	7	7	0	60	77	01
3	2	3	00	07	11	5	1	2	00	37	41	7	0	1	00	67	71
2	3	3	00	70	70	4	2	2	00	20	20	6	1	1	00	50	50
3	4	3	20	01	77	5	3	2	20	31	27	7	2	1	20	61	57
2	5	3	20	72	56	4	4	2	20	22	06	6	3	1	20	52	36
3	6	3	40	03	55	5	5	2	40	33	05	7	4	1	40	63	35
2	7	3	40	74	34	4	6	2	40	24	64	6	5	1	40	54	14
2	0	4	60	64	24	5	7	2	60	35	63	7	6	1	60	65	13
3	1	4	00	75	23	5	0	3	00	25	53	6	7	1	60	56	72
2	2	4	00	66	02	4	1	3	00	16	32	6	0	2	00	46	62
3	3	4	20	77	01	5	2	3	20	27	31	7	1	2	20	57	61
2	4	4	20	60	60	4	3	3	20	10	10	6	2	2	20	40	40
3	5	4	40	71	67	5	4	3	40	21	17	7	3	2	40	51	47
2	6	4	40	62	46	4	5	3	40	12	76	6	4	2	40	42	26
3	7	4	60	73	45	5	6	3	60	23	75	7	5	2	60	53	25
3	0	5	00	63	35	4	7	3	60	14	54	6	6	2	60	44	04
2	1	5	00	54	14	4	0	4	00	04	44	7	7	2	00	55	03
3	2	5	20	65	13	5	1	4	20	15	43	7	0	3	20	45	73
2	3	5	20	56	72	4	2	4	20	06	22	6	1	3	20	36	52
3	4	5	40	67	71	5	3	4	40	17	21	7	2	3	40	47	51
2	5	5	40	50	50	4	4	4	40	00	00	6	3	3	40	30	30
3	6	5	60	61	57	5	5	4	60	11	07	7	4	3	60	41	37
2	7	5	60	52	36	4	6	4	60	02	66	6	5	3	60	32	16
2	0	6	00	42	26	5	7	4	00	13	65	7	6	3	00	43	15
3	1	6	20	53	25	5	0	5	20	03	55	6	7	3	00	34	74
2	2	6	20	44	04	4	1	5	20	74	34	6	0	4	20	24	64
3	3	6	40	55	03	5	2	5	40	05	33	7	1	4	40	35	63
2	4	6	40	46	62	4	3	5	40	76	12	6	2	4	40	26	42
3	5	6	60	57	61	5	4	5	60	07	11	7	3	4	60	37	41
6	4	4	60	20	20	1	4	3	00	61	57	0	3	3	60	50	50
7	5	4	00	31	27	0	5	3	00	52	36	1	2	3	60	67	71
6	6	4	00	22	06	1	6	3	20	63	35	1	0	3	40	65	13
0	1	3	40	56	72	1	0	1	20	07	11	0	7	7	60	10	10
7	7	4	20	33	05	0	7	3	20	54	14	1	7	2	20	75	23
7	0	5	40	23	75	0	0	4	40	44	04	0	1	1	20	70	70
1	2	1	40	01	77	0	3	1	40	72	56	1	4	1	60	03	55
0	5	1	60	74	34	1	6	1	00	05	33	0	7	1	00	76	12
0	0	2	20	66	02	1	1	2	40	77	01	0	2	2	40	60	60
1	3	2	60	71	67	0	4	2	60	62	46	1	5	2	00	73	45
0	6	2	00	64	24	6	1	5	40	14	54	1	1	4	60	55	03
7	2	5	60	25	53	0	2	4	60	46	62	1	3	4	00	57	61
6	3	5	60	16	32	7	4	5	00	27	31	0	4	4	00	40	40
6	5	5	00	10	10	1	5	4	20	51	47	0	6	4	20	42	26
7	6	5	20	21	17	6	7	5	20	12	76	1	7	4	40	53	25
6	0	6	40	02	66	1	0	5	60	43	15	0	1	5	60	34	74
7	1	6	60	13	65	6	2	6	60	04	44	1	2	5	00	45	73
7	3	6	00	15	43	0	3	5	00	36	52	1	4	5	20	47	51

(continued..)

6 4 6	00 06 22	7 5 6	20 17 21	0 5 5	20 30 30
6 6 6	20 00 00	1 6 5	40 41 37	0 7 5	40 32 16
7 7 6	40 11 07	7 0 7	60 01 77	0 0 6	60 22 06
6 1 7	60 72 56	1 1 6	00 33 05	0 2 6	00 24 64
7 2 7	00 03 55	6 3 7	00 74 34	1 3 6	20 35 63
7 4 7	20 05 33	0 4 6	20 26 42	1 5 6	40 37 41
6 5 7	20 76 12	7 6 7	40 07 11	0 6 6	40 20 20
6 7 7	40 70 70	1 7 6	60 31 27	1 0 7	00 21 17
1 1 0	20 11 07	0 2 0	20 02 66	0 1 7	00 12 76
1 3 0	40 13 65	1 2 7	20 23 75	0 3 7	20 14 54
0 4 0	40 04 44	1 5 0	60 15 43	1 4 7	40 25 53
0 6 0	60 06 22	0 5 7	40 16 32	1 6 7	60 27 31
1 7 0	00 17 21				

APPENDIX B

LISTING OF ALL SELF-DUAL CODES OF LENGTH 7 OVER Z_4

In this appendix codewords and their spectrum of all the three self-dual codes corresponding to Example 6.3 are listed.

Code 1: The conjugacy classes $C_{2,7}(1)$ and $C_{2,7}(3)$ take values from ideal 2GR(4,3).

codeword							spectrum							codeword							spectrum						
a_0	a_1	a_2	a_3	a_4	a_5	a_6	A_0	A_1	A_2	A_3	A_4	A_5	A_6	a_0	a_1	a_2	a_3	a_4	a_5	a_6	A_0	A_1	A_2	A_3	A_4	A_5	A_6
0	0	0	0	0	0	0	000	000	000	000	000	000	000	2	0	0	0	0	0	0	200	200	200	200	200	200	200
0	0	2	0	0	0	0	200	022	020	222	002	202	220	2	2	2	0	0	0	0	200	220	202	220	222	222	202
0	2	0	2	0	0	0	000	200	200	220	200	222	202	2	0	2	2	0	0	0	200	020	002	000	022	000	000
0	0	0	0	2	0	0	200	020	002	220	022	222	202	2	2	0	0	2	0	0	200	222	220	222	202	202	220
0	2	2	0	2	0	0	200	000	000	200	000	200	200	2	0	0	2	2	0	0	200	022	020	002	002	020	022
0	0	2	2	2	0	0	200	200	200	020	200	022	002	2	2	2	2	2	0	0	200	002	022	022	020	002	020
0	2	0	0	0	2	0	000	222	220	200	202	200	200	2	0	2	0	0	2	0	200	002	022	020	020	022	002
0	0	0	2	0	2	0	000	022	020	020	002	022	002	2	2	0	2	0	2	0	000	220	202	022	222	002	020
0	2	2	2	0	2	0	000	002	022	000	020	000	000	2	0	0	0	2	2	0	200	000	000	022	000	002	020
0	0	2	0	2	2	0	200	222	220	000	202	000	000	2	2	0	0	0	0	0	200	002	022	202	020	220	222
2	0	2	0	0	0	0	000	222	220	022	202	002	020	0	0	0	2	0	0	0	200	202	222	022	220	002	020
2	2	0	2	0	0	0	200	000	000	020	000	022	002	0	2	2	2	0	0	0	200	222	220	002	202	020	022
2	0	0	0	2	0	0	000	220	202	020	222	022	002	0	0	2	0	2	0	0	000	002	022	002	020	020	022
2	2	2	0	2	0	0	000	200	200	000	200	000	000	0	2	0	2	2	0	0	200	220	202	000	222	000	000
2	0	2	2	2	0	0	000	000	000	220	000	222	202	0	0	0	0	0	2	0	200	220	202	002	222	020	022
2	2	0	0	0	2	0	200	022	020	000	002	000	000	0	2	2	0	0	2	0	200	200	200	022	200	002	020
2	0	0	2	0	2	0	200	222	220	220	202	222	202	0	0	2	2	0	2	0	200	000	000	202	000	220	222
2	2	2	2	0	2	0	200	202	222	200	220	200	200	0	2	0	0	2	2	0	200	202	222	020	220	022	002
2	0	2	0	2	2	0	000	022	020	200	002	200	200	2	2	0	0	0	0	0	000	202	222	002	220	020	022
0	2	2	0	0	0	0	000	020	002	020	022	022	002	2	0	0	2	0	0	0	000	002	022	222	020	202	022
0	0	2	2	0	0	0	000	220	202	200	222	200	200	2	2	2	2	0	0	0	000	022	020	202	002	220	222
0	2	0	0	2	0	0	000	022	020	022	002	002	020	2	0	2	0	2	0	0	200	202	222	202	220	220	222
0	0	0	2	2	0	0	000	222	220	202	202	220	222	2	2	0	2	2	0	0	000	020	002	200	022	200	200
0	2	2	2	2	0	0	000	202	222	222	220	202	220	2	0	0	0	0	2	0	000	020	002	202	022	220	222
0	0	2	0	0	2	0	000	202	222	220	220	222	202	2	2	2	0	0	2	0	000	000	000	222	000	202	220
0	2	0	2	0	2	0	200	020	002	222	022	202	220	2	0	2	2	0	2	0	000	200	200	002	200	020	022
0	0	0	0	2	2	0	000	200	200	222	200	202	220	2	2	0	0	2	2	0	000	002	022	220	020	222	202
0	2	2	0	2	2	0	000	220	202	202	222	220	222	2	2	2	0	2	2	0	200	020	002	002	022	020	022
0	2	0	2	2	2	0	000	000	000	002	000	020	022	2	0	2	2	2	2	0	200	220	202	222	222	202	220
0	0	0	0	0	0	2	200	222	220	020	202	022	002	2	2	0	0	0	0	2	200	020	002	022	022	002	020
0	2	2	0	0	0	2	200	202	222	000	220	000	000	2	0	0	2	0	0	2	200	220	202	202	222	220	222
0	0	2	2	0	0	2	200	002	022	220	020	222	202	2	2	2	2	0	0	2	200	200	200	222	200	202	220
0	2	0	0	2	0	2	200	200	200	002	200	020	022	2	0	2	0	2	0	2	000	020	002	222	022	202	220
0	0	0	2	2	0	2	200	000	000	222	000	202	220	2	2	0	2	2	0	2	200	202	222	220	220	222	202
0	2	2	2	2	0	2	200	020	002	202	022	220	222	2	0	0	0	0	2	2	200	202	222	222	220	202	220

(continued..)

| | | |

| | | |

code 3: The conjugacy class $C_{2,7}(1)$ takes values from the ideal $2^0GR(4,3)$ and the conjugacy class $C_{2,7}(3)$ from $2^2GR(4,3)$.

codeword							spectrum							codeword							spectrum						
a_0	a_1	a_2	a_3	a_4	a_5	a_6	A_0	A_1	A_2	A_3	A_4	A_5	A_6	a_0	a_1	a_2	a_3	a_4	a_5	a_6	A_0	A_1	A_2	A_3	A_4	A_5	A_6
0	0	0	0	0	0	0	000	000	000	000	000	000	000	2	0	2	2	0	0	0	200	020	002	000	022	000	000
2	2	2	0	2	0	0	000	200	200	000	200	000	000	3	3	1	2	3	0	0	000	320	302	000	322	000	000
3	0	2	1	1	1	0	000	101	133	000	310	000	000	0	1	1	3	2	1	0	000	221	231	000	032	000	000
2	2	0	0	0	2	0	200	022	020	000	002	000	000	3	3	3	2	1	2	0	200	102	122	000	120	000	000
3	1	3	0	3	2	0	000	322	320	000	302	000	000	0	1	3	3	0	3	0	200	003	011	000	230	000	000
0	3	3	1	2	3	0	000	223	213	000	012	000	000	1	0	2	3	3	3	0	000	303	311	000	130	000	000
0	0	3	1	1	0	1	200	033	210	000	001	000	000	1	1	2	3	2	0	1	200	113	312	000	123	000	000
3	2	1	0	0	1	1	000	310	101	000	133	000	000	0	3	0	2	1	1	1	000	030	203	000	211	000	000
0	1	0	0	3	1	1	200	210	001	000	033	000	000	1	1	0	3	0	2	1	000	331	132	000	321	000	000
1	3	0	1	2	2	1	200	111	330	000	103	000	000	2	0	3	3	3	2	1	200	231	032	000	221	000	000
0	1	2	0	1	3	1	000	032	221	000	231	000	000	1	2	1	2	2	3	1	000	112	323	000	313	000	000
0	2	2	0	0	0	2	200	202	222	000	220	000	000	3	1	1	0	1	0	0	200	100	100	000	100	000	000
0	2	0	2	2	0	0	200	220	202	000	222	000	000	0	3	1	1	0	1	0	200	001	033	000	210	000	000
1	0	0	3	1	1	0	200	121	131	000	332	000	000	1	2	0	1	3	1	0	000	301	333	000	110	000	000
0	2	2	2	0	2	0	000	002	022	000	020	000	000	0	0	2	0	2	2	0	200	222	220	000	202	000	000
1	1	1	2	3	2	0	200	302	322	000	320	000	000	1	2	2	1	1	3	0	200	123	113	000	312	000	000
2	3	1	3	2	3	0	200	203	211	000	030	000	000	1	3	2	1	0	0	1	000	333	110	000	301	000	000
2	0	1	3	1	0	1	000	013	212	000	023	000	000	2	2	1	1	3	0	1	200	233	010	000	201	000	000
1	2	3	2	0	1	1	200	330	103	000	111	000	000	1	0	3	0	2	1	1	000	110	301	000	333	000	000
2	1	2	2	3	1	1	000	230	003	000	011	000	000	2	2	3	1	1	2	1	000	011	230	000	003	000	000
3	3	2	3	2	2	1	000	131	332	000	121	000	000	1	0	1	0	0	3	1	200	332	121	000	131	000	000
2	1	0	2	1	3	1	200	012	223	000	213	000	000	2	3	0	0	3	3	1	000	232	021	000	031	000	000
2	2	0	2	0	0	2	000	222	220	000	202	000	000	1	1	3	2	1	0	0	000	120	102	000	122	000	000
1	3	3	0	3	0	0	200	300	300	000	300	000	000	2	3	3	3	0	1	0	000	021	031	000	232	000	000
2	1	3	1	2	1	0	200	201	233	000	010	000	000	3	2	2	3	3	1	0	200	321	331	000	132	000	000
1	3	1	0	1	2	0	000	122	120	000	102	000	000	2	0	0	2	2	2	0	000	202	222	000	220	000	000
2	1	1	1	0	3	0	000	023	013	000	212	000	000	3	2	0	3	1	3	0	000	103	111	000	330	000	000
3	0	0	1	3	3	0	200	323	313	000	112	000	000	3	3	0	3	0	0	1	200	313	112	000	323	000	000
3	1	0	1	2	0	1	000	133	310	000	101	000	000	0	2	3	3	3	0	1	000	213	012	000	223	000	000
2	3	2	0	1	1	1	200	010	201	000	233	000	000	3	0	1	2	2	1	1	200	130	303	000	311	000	000
3	1	2	1	0	2	1	200	311	130	000	303	000	000	0	2	1	3	1	2	1	200	031	232	000	021	000	000
0	0	1	1	3	2	1	000	211	030	000	203	000	000	3	0	3	2	0	3	1	000	312	123	000	113	000	000
3	2	3	0	2	3	1	200	132	321	000	331	000	000	0	3	2	2	3	3	1	200	212	023	000	013	000	000
3	3	3	0	1	0	2	000	302	322	000	320	000	000	1	3	1	2	1	0	2	200	322	320	000	302	000	000
1	1	1	0	3	0	2	000	102	122	000	120	000	000	2	1	1	3	0	1	2	200	223	213	000	012	000	000
2	3	1	1	2	1	2	000	003	011	000	230	000	000	3	0	0	3	3	1	2	000	123	113	000	312	000	000
1	1	3	0	1	2	2	200	320	302	000	322	000	000	2	2	2	2	2	2	2	200	000	000	000	000	000	000
2	3	3	1	0	3	2	200	221	231	000	032	000	000	3	0	2	3	1	3	2	200	301	333	000	110	000	000
3	2	2	1	3	3	2	000	121	131	000	332	000	000	3	1	2	3	0	0	3	000	111	330	000	103	000	000
3	3	2	1	2	0	3	200	331	132	000	321	000	000	0	0	1	3	3	0	3	200	011	230	000	003	000	000
2	1	0	0	1	1	3	000	212	023	000	013	000	000	3	2	3	2	2	1	3	000	332	121	000	131	000	000
3	3	0	1	0	2	3	000	113	312	000	123	000	000	0	0	3	3	1	2	3	000	233	010	000	201	000	000

(continued..)

| | | |

APPENDIX C

LISTING OF MINIMUM HAMMING AND LEE DISTANCES AND NUMBER OF CODEWORDS OF ALL CYCLIC CODES FOR DIFFERENT VALUES OF n AND p^k.

In this appendix the minimum Hamming and Lee distance and the number of codewords for all cyclic codes for the following values of n and p^k are listed.

(1) n=4 ; p^k = 4

(2) n=5 ; p^k = 4

(3) n=7 ; p^k = 4

(4) n=4 ; p^k = 9

(5) n=3 ; p^k = 8

For the sake of completeness the 'codes' consisting of all the n-tuples and consisting of only zero vector is also included. In all the cases,

H denotes the minimum Hamming distance

L denotes the minimum Lee distance

M denotes the total number of codewords.

(1) Z_4; n=3

Conjugacy class $C_{2,3}(0) = \{ 0 \}$ takes value from $2^{j_1}GR(4,1)$ and conjugacy class $C_{2,3}(1) = \{ 1,2 \}$ takes value from $2^{j_2}GR(4,2)$. Any cyclic code is of the form $2^{j_1}GR(4,1) \oplus 2^{j_2}GR(4,2)$, where $j_1, j_2 = 0,1,2$.

j_1	j_2	H	L	M
2	2	0	0	1
2	1	2	4	4
2	0	2	2	16
1	2	3	6	2
1	1	1	2	8
1	0	1	2	32
0	2	3	3	4
0	1	1	2	16
0	0	1	1	64

(2) Z_4; n=5

Conjugacy class {0} takes value from $2^{j_1}GR(4,1)$ and conjugacy class {1,2,3,4} takes value from $2^{j_2}GR(4,4)$. Any cyclic code is of the form $2^{j_1}GR(4,1) \oplus 2^{j_2}GR(4,4)$, where $j_1, j_2 = 0,1,2$.

j_1	j_2	H	L	M
2	2	0	0	1
2	1	2	4	16
2	0	2	2	256
1	2	5	10	2
1	1	1	2	32
1	0	1	2	512
0	2	5	5	4
0	1	1	2	64
0	0	1	1	1024

(3) Z_4; n=7

Conjugacy class (0) takes value from $2^{j_1}GR(4,1)$,
conjugacy class (1,2,4) takes value from $2^{j_2}GR(4,3)$ and
conjugacy class (3,5,6) takes value from $2^{j_3}GR(4,3)$.
Any cyclic code is of the form

$$2^{j_1}GR(4,1) \oplus 2^{j_2}GR(4,3) \oplus 2^{j_3}GR(4,3)$$ where

$j_1, j_2, j_3 = 0,1,2$.

j_1	j_2	j_3	H	L	M
2	2	2	0	0	1
2	2	1	4	8	8
2	2	0	4	6	64
2	1	2	4	8	8
2	1	1	2	4	64
2	1	0	2	4	512
2	0	2	4	6	64
2	0	1	2	4	512
2	0	0	2	2	4096
1	2	2	7	14	2
1	2	1	3	6	16
1	2	0	3	4	128
1	1	2	3	6	16
1	1	1	1	2	28
1	1	0	1	2	1024
1	0	2	3	4	128
1	0	1	1	1	1024
1	0	0	1	2	8192
0	2	2	7	7	4
0	2	1	3	6	32
0	2	0	3	4	256
0	1	2	3	6	32
0	1	1	1	2	156
0	1	0	1	2	2048
0	0	2	3	4	256
0	0	1	1	2	2048
0	0	0	1	1	16384

(4) Z_9; n=4

Conjugacy class (0) takes value from $3^{j_1}GR(9,1)$,
conjugacy class (1,3) takes value from $3^{j_2}GR(9,2)$ and
conjugacy class (2) takes value from $3^{j_3}GR(9,1)$.
Any cyclic code is of the form

$$3^{j_1}GR(9,1) \oplus 3^{j_2}GR(9,2) \oplus 3^{j_3}GR(9,1)$$ where

$j_1, j_2, j_3 = 0,1,2$.

j_1	j_2	j_3	H	L	M
2	2	2	0	0	1
2	2	1	4	12	3
2	2	0	4	4	9
2	1	2	2	6	9
2	1	1	2	6	27
2	1	0	2	4	81
2	0	2	2	2	81
2	0	1	2	2	243
2	0	0	2	2	729
1	2	2	4	12	3
1	2	1	2	6	9
1	2	0	2	6	27
1	1	2	2	6	27
1	1	1	1	3	81
1	1	0	1	3	243
1	0	2	2	2	243
1	0	1	1	2	729
1	0	0	1	2	2187
0	2	2	4	4	9
0	2	1	2	6	27
0	2	0	2	2	81
0	1	2	2	4	81
0	1	1	1	3	243
0	1	0	1	2	729
0	0	2	2	2	729
0	0	1	1	2	2187
0	0	0	1	1	6561

(5) Z_8; n=3

Conjugacy class (0) takes value from $2^{j_1}GR(8,1)$ and conjugacy class (1,2) takes value from $2^{j_2}GR(8,2)$. Any cyclic code is of the form $2^{j_1}GR(8,1) \oplus 2^{j_2}GR(8,2)$, where $j_1, j_2 = 0,1,2,3$.

j_1	j_2	H	L	M
3	3	0	0	1
3	2	2	8	4
3	1	2	4	16
3	0	2	2	64
2	3	3	12	2
2	2	1	4	8
2	1	1	4	32
2	0	1	2	128
1	3	3	6	4
1	2	1	4	16
1	1	1	2	64
1	0	1	2	256
0	3	3	3	8
0	2	1	3	32
0	1	1	2	128
0	0	1	1	512

APPENDIX D

LISTING OF CODEWORDS AND SPECTRUM CORRESPONDING TO EXAMPLE 4.11

codeword	spectrum				
2 0 0 0 0	2000	2000	2000	2000	2000
2 4 0 0 0	0000	2020	4402	0420	4424
2 2 2 0 0	0000	0244	4440	4220	2422
2 0 4 0 0	0000	4402	4424	2020	0420
2 4 4 0 0	4000	4422	0220	0440	2244
2 2 0 2 0	0000	4220	0244	2422	4440
2 0 2 2 0	0000	2444	0222	0222	2444
2 4 2 2 0	4000	2404	2024	4042	4202
2 2 4 2 0	4000	0022	2002	2442	2200
2 0 0 4 0	0000	0420	2020	4424	4402
2 4 0 4 0	4000	0440	4422	2244	0220
2 2 2 4 0	4000	4004	4400	0044	4224
2 0 4 4 0	4000	2222	4444	4444	2222
2 4 4 4 0	2000	2242	0240	2204	4040
3 3 1 1 1	3000	2040	0204	4240	0242
3 1 3 1 1	3000	0204	0242	2040	4240
3 5 3 1 1	1000	0224	2044	0400	0004
3 3 5 1 1	1000	4442	2022	4200	4002
3 1 1 3 1	3000	4240	2040	0242	0204
3 5 1 3 1	1000	4200	4442	4002	2022
3 3 3 3 1	1000	2424	4420	2402	0020
3 1 5 3 1	1000	0042	4404	0202	4024
3 5 5 3 1	5000	0002	0200	4022	0442
3 3 1 5 1	1000	0400	0224	0004	2044
3 1 3 5 1	1000	4024	0202	4404	0042
3 5 3 5 1	5000	4044	2004	2224	2400
3 3 5 5 1	5000	2202	2042	0024	0404
2 0 0 0 2	4000	0242	4240	0204	2040
2 4 0 0 2	2000	0202	0042	4024	4404
2 2 2 0 2	2000	4420	0020	2424	2402
2 0 4 0 2	2000	2044	0004	0224	0400
2 4 4 0 2	0000	2004	2400	4044	2224
2 2 0 2 2	2000	2402	2424	0020	4420
2 0 2 2 2	2000	0020	2402	4420	2424
2 4 2 2 2	0000	0040	4204	2240	4242
2 2 4 2 2	0000	4204	4242	0040	2240
2 0 0 4 2	2000	4002	4200	2022	4442
2 4 0 4 2	0000	4022	0002	0442	0200
2 2 2 4 2	0000	2240	0040	4242	4204
2 0 4 4 2	0000	0404	0024	2042	2202
2 4 4 4 2	4000	0424	2420	0402	4020
3 3 1 1 3	5000	0222	2444	2444	0222
3 1 3 1 3	5000	4440	2422	0244	4220
3 5 3 1 3	3000	4400	4224	4004	0044

codeword	spectrum				
2 2 0 0 0	4000	2040	0204	4240	0242
2 0 2 0 0	4000	0204	0242	2040	4240
2 4 2 0 0	2000	0224	2044	0400	0004
2 2 4 0 0	2000	4442	2022	4200	4002
2 0 0 2 0	4000	4240	2040	0242	0204
2 4 0 2 0	2000	4200	4442	4002	2022
2 2 2 2 0	2000	2424	4420	2402	0020
2 0 4 2 0	2000	0042	4404	0202	4024
2 4 4 2 0	0000	0002	0200	4022	0442
2 2 0 4 0	2000	0400	0224	0004	2044
2 0 2 4 0	2000	4024	0202	4404	0042
2 4 2 4 0	0000	4044	2004	2224	2400
2 2 4 4 0	0000	2203	2042	0024	0404
3 1 1 1 1	1000	2000	2000	2000	2000
3 5 1 1 1	5000	2020	4402	0420	4424
3 3 3 1 1	5000	0244	4440	4220	2422
3 1 5 1 1	5000	4402	4424	2020	0420
3 5 5 1 1	3000	4422	0220	0440	2244
3 3 1 3 1	5000	4220	0244	2422	4440
3 1 3 3 1	5000	2444	0222	0222	2444
3 5 3 3 1	3000	2404	2024	4042	4202
3 3 5 3 1	3000	0022	2002	2442	2200
3 1 1 5 1	5000	0420	2020	4424	4402
3 5 1 5 1	3000	0440	4422	2244	0220
3 3 3 5 1	3000	4004	4400	0044	4224
3 1 5 5 1	3000	2222	4444	4444	2222
3 5 5 5 1	1000	2242	0240	2204	4040
2 2 0 0 2	0000	0222	2444	2444	0222
2 0 2 0 2	0000	4440	2422	0244	4220
2 4 2 0 2	4000	4400	4224	4004	0044
2 2 4 0 2	4000	2024	4202	2404	4042
2 0 0 2 2	0000	2422	4220	4440	0244
2 4 0 2 2	4000	2442	0022	2200	2002
2 2 2 2 2	4000	0000	0000	0000	0000
2 0 4 2 2	4000	4224	0044	4400	4004
2 4 4 2 2	2000	4244	2440	2220	0422
2 2 0 4 2	4000	4042	2404	4202	2024
2 0 2 4 2	4000	2200	2442	2002	0022
2 4 2 4 2	2000	2220	4244	0422	2440
2 2 4 4 2	2000	0444	4222	4222	0444
3 1 1 1 3	3000	0242	4240	0204	2040
3 5 1 1 3	1000	0202	0042	4024	4404
3 3 3 1 3	1000	4420	0020	2424	2402
3 1 5 1 3	1000	2044	0004	0224	0400

(continued..)

3 3 5 1 3	3000	2024	4202	2404	4042
4 2 0 0 0	0000	4040	2204	0240	2242
4 0 2 0 0	0000	2204	2242	4040	0240
4 4 2 0 0	4000	2224	4044	2400	2004
4 2 4 0 0	4000	0442	4022	0200	0002
4 0 0 2 0	0000	0240	4040	2242	2204
4 4 0 2 0	4000	0200	0442	0002	4022
4 2 2 2 0	4000	4424	0420	4402	2020
4 0 4 2 0	4000	2042	0404	2202	0024
4 4 4 2 0	2000	2002	2200	0022	2442
4 2 0 4 0	4000	2400	2224	2004	4044
4 0 2 4 0	4000	0024	2202	0404	2042
4 4 2 4 0	2000	0044	4004	4224	4400
4 2 4 4 0	2000	4202	4042	2024	2404
5 1 1 1 1	3000	4000	4000	4000	4000
5 5 1 1 1	1000	4020	0402	4240	0424
5 3 3 1 1	1000	2244	0440	0220	4422
5 1 5 1 1	1000	0402	0424	4020	2420
5 5 5 1 1	5000	0422	2220	2440	4244
5 3 1 3 1	1000	0220	2244	4422	0440
5 1 3 3 1	1000	4444	2222	2222	4444
5 5 3 3 1	5000	4404	4024	0042	0202
5 3 5 3 1	5000	2022	4002	4442	4200
5 1 1 5 1	1000	2420	4020	0424	0402
5 5 1 5 1	5000	2440	0422	4244	2220
5 3 3 5 1	5000	0004	0400	2044	0224
5 1 5 5 1	5000	4222	0444	0444	4222
5 5 5 5 1	3000	4242	2240	4204	0040
4 2 0 0 2	2000	2222	4444	4444	2222
4 0 2 0 2	2000	0440	4422	2244	0220
4 4 2 0 2	0000	0400	0224	0004	2044
4 2 4 0 2	0000	4024	0202	4404	0042
4 0 0 2 2	2000	4422	0220	0440	2244
4 4 0 2 2	0000	4442	2022	4200	4002
4 2 2 2 2	0000	2000	2000	2000	2000
4 0 4 2 2	0000	0224	2044	0400	0004
4 4 4 2 2	4000	0244	4440	4220	2422
4 2 0 4 2	0000	0042	4404	0202	4024
4 0 2 4 2	0000	4200	4442	4002	2022
4 4 2 4 2	4000	4220	0244	2422	4440
4 2 4 4 2	4000	2444	0222	0222	2444
5 1 1 1 3	5000	2242	0240	2204	4040
5 5 1 1 3	3000	2202	2042	0024	0404
5 3 3 1 3	3000	0420	2020	4424	4402
5 1 5 1 3	3000	4044	2004	2224	2400
0 2 0 0 0	2000	0040	4204	2240	4242
0 0 2 0 0	2000	4204	4242	0040	2240
0 4 2 0 0	0000	4224	0044	4400	4004
0 2 4 0 0	0000	2442	0022	2200	2002
0 0 0 2 0	2000	2240	0040	4242	4204
0 4 0 2 0	0000	2200	2442	2002	0022

4 0 0 0 0	4000	4000	4000	4000	4000
4 4 0 0 0	2000	4020	0402	2420	0424
4 2 2 0 0	2000	2244	0440	0220	4422
4 0 4 0 0	2000	0402	0424	4020	2420
4 4 4 0 0	0000	0422	2220	2440	4244
4 2 0 2 0	2000	0220	2244	4422	0440
4 0 2 2 0	2000	4444	2222	2222	4444
4 4 2 2 0	0000	4404	4024	0042	0202
4 2 4 2 0	0000	2022	4002	4442	4200
4 0 0 4 0	2000	2420	4020	0424	0402
4 4 0 4 0	0000	2440	0422	4244	2220
4 2 2 4 0	0000	0004	0400	2044	0224
4 0 4 4 0	0000	4222	0444	0444	4222
4 4 4 4 0	4000	4242	2240	4204	0040
5 3 1 1 1	5000	4040	2204	0240	2242
5 1 3 1 1	5000	2204	2242	4040	0240
5 5 3 1 1	3000	2224	4044	2400	2004
5 3 5 1 1	3000	0442	4022	0200	0002
5 1 1 3 1	5000	0240	4040	2242	2204
5 5 1 3 1	3000	0200	0442	0002	4022
5 3 3 3 1	3000	4424	0420	4402	2020
5 1 5 3 1	3000	2042	0404	2202	0024
5 5 5 3 1	1000	2002	2200	0022	2442
5 3 1 5 1	3000	2400	2224	2004	4044
5 1 3 5 1	3000	0024	2202	0404	2042
5 5 3 5 1	1000	0044	4004	4224	4400
5 3 5 5 1	1000	4202	4042	2024	2404
4 0 0 0 2	0000	2242	0240	2204	4040
4 4 0 0 2	4000	2202	2042	0024	0404
4 2 2 0 2	4000	0420	2020	4424	4402
4 0 4 0 2	4000	4044	2004	2224	2400
4 4 4 0 2	2000	4004	4400	0044	4224
4 2 0 2 2	4000	4402	4424	2020	0420
4 0 2 2 2	4000	2020	4402	0420	4424
4 4 2 2 2	2000	2040	0204	4240	0242
4 2 4 2 2	2000	0204	0242	2040	4240
4 0 0 4 2	4000	0002	0200	4022	0442
4 4 0 4 2	2000	0022	2002	2442	2200
4 2 2 4 2	2000	4240	2040	0242	0204
4 0 4 4 2	2000	2404	2024	4042	4202
4 4 4 4 2	0000	2424	4420	2402	0020
5 3 1 1 3	1000	2222	4444	4444	2222
5 1 3 1 3	1000	0440	4422	2244	0220
5 5 3 1 3	5000	0400	0224	0004	2044
5 3 5 1 3	5000	4224	0002	4404	0042
0 4 0 0 0	4000	0020	2402	4420	2424
0 2 2 0 0	4000	4244	2440	2220	0422
0 0 4 0 0	4000	2402	2424	0020	4420
0 4 4 0 0	2000	2422	4220	4440	0244
0 2 0 2 0	4000	2220	4244	0422	2440
0 0 2 2 0	4000	0444	4222	4222	0444

(continued..)

0 2 2 2 0	0000	0424	2420	0402	4020
0 0 4 2 0	0000	4042	2404	4202	2024
0 4 4 2 0	4000	4002	4200	2022	4442
0 2 0 4 0	0000	4400	4224	4004	0044
0 0 2 4 0	0000	2024	4202	2404	4042
0 4 2 4 0	4000	2044	0004	0224	0400
0 2 4 4 0	4000	0202	0042	4024	4404
1 1 1 1 1	5000	0000	0000	0000	0000
1 5 1 1 1	3000	0020	2402	4420	2424
1 3 3 1 1	3000	4244	2440	2220	0422
1 1 5 1 1	3000	2402	2424	0020	4420
1 5 5 1 1	1000	2422	4220	4440	0244
1 3 1 3 1	3000	2220	4244	0422	2440
1 1 3 3 1	3000	0444	4222	4222	0444
1 5 3 3 1	1000	0404	0024	2042	2202
1 3 5 3 1	1000	4022	0002	0442	0200
1 1 1 5 1	3000	4420	0020	2424	2402
1 5 1 5 1	1000	4440	2422	0244	4220
1 3 3 5 1	1000	2004	2400	4044	2224
1 1 5 5 1	1000	0222	2444	2444	0222
1 5 5 5 1	5000	0242	4240	0204	2040
0 2 0 0 2	4000	4222	0444	0444	4222
0 0 2 0 2	4000	2440	0422	4244	2220
0 4 2 0 2	2000	2400	2224	2004	4044
0 2 4 0 2	2000	0024	2202	0404	2042
0 0 0 2 2	4000	0422	2220	2440	4244
0 4 0 2 2	2000	0442	4022	0200	0002
0 2 2 2 2	2000	4000	4000	4000	4000
0 0 4 2 2	2000	2224	4044	2400	2004
0 4 4 2 2	0000	2244	0440	0220	4422
0 2 0 4 2	2000	2042	0404	2202	0024
0 0 2 4 2	2000	0200	0442	0002	4022
0 4 2 4 2	0000	0220	2244	4422	0440
0 2 4 4 2	0000	4444	2222	2222	4444
1 1 1 1 3	1000	4242	2240	4204	0040
1 5 1 1 3	5000	4202	4042	2024	2404
1 3 3 1 3	5000	2420	4020	0424	0402
1 1 5 1 3	5000	0044	4004	4224	4400
1 5 5 1 3	3000	0024	0400	2044	2224
3 1 1 3 3	5000	2422	4220	4440	0244
3 5 1 3 3	3000	2442	0022	2200	2002
3 3 3 3 3	3000	0000	0000	0000	0000
3 1 5 3 3	3000	4224	0044	4400	4004
3 5 5 3 3	1000	4244	2440	2220	0422
3 3 1 5 3	3000	4042	2404	4202	2024
3 1 3 5 3	3000	2200	2442	2002	0022
3 5 3 5 3	1000	2220	4244	0422	2440
3 3 5 5 3	1000	0444	4222	4222	0444
2 0 0 0 4	0000	4424	0420	4402	2020
2 4 0 0 4	4000	4444	2222	2222	4444
2 2 2 0 4	4000	2002	2200	0022	2442
0 4 2 2 0	2000	0404	0024	2042	2202
0 2 4 2 0	2000	4022	0002	0442	0200
0 0 0 4 0	4000	4420	0020	2424	2402
0 4 0 4 0	2000	4440	2422	0244	4220
0 2 2 4 0	2000	2004	2400	4044	2224
0 0 4 4 0	2000	0222	2444	2444	0222
0 4 4 4 0	0000	0242	4240	0204	2040
1 3 1 1 1	1000	0040	4204	2240	4242
1 1 3 1 1	1000	4204	4242	0040	2240
1 5 3 1 1	5000	4224	0044	4400	4004
1 3 5 1 1	5000	2442	0022	2200	2002
1 1 1 3 1	1000	2240	0040	4242	4204
1 5 1 3 1	5000	2200	2442	2002	0022
1 3 3 3 1	5000	0424	2420	0402	4020
1 1 5 3 1	5000	4042	2404	4202	2024
1 5 5 3 1	3000	4002	4200	2022	4442
1 3 1 5 1	5000	4400	4224	4004	0044
1 1 3 5 1	5000	2024	4202	2404	4042
1 5 3 5 1	3000	2044	0004	0224	0400
1 3 5 5 1	3000	0202	0042	4024	4404
0 0 0 0 2	2000	4242	2240	4204	0040
0 4 0 0 2	0000	4202	4042	2024	2404
0 2 2 0 2	0000	2420	4020	0424	0402
0 0 4 0 2	0000	0044	4004	4224	4400
0 4 4 0 2	4000	0004	0400	2044	0224
0 2 0 2 2	0000	0402	0424	4020	2420
0 0 2 2 2	0000	4020	0402	2420	0424
0 4 2 2 2	4000	4040	2204	0240	2242
0 2 4 2 2	4000	2204	2242	4040	0240
0 0 0 4 2	0000	2002	2200	0022	2442
0 4 0 4 2	4000	2022	4002	4442	4200
0 2 2 4 2	4000	0240	4040	2242	2204
0 0 4 4 2	4000	4404	4024	0042	0202
0 4 4 4 2	2000	4424	0420	4402	2020
1 3 1 1 3	3000	4222	0444	0444	4222
1 1 3 1 3	3000	1440	0422	4244	2220
1 5 3 1 3	1000	2400	2224	2004	4044
1 3 5 1 3	1000	0024	2202	0404	2042
3 5 5 1 3	5000	2004	2400	4044	2224
3 3 1 3 3	1000	2402	2424	0020	4420
3 1 3 3 3	1000	0020	2402	4420	2424
3 5 3 3 3	5000	0040	4204	2240	4242
3 3 5 3 3	5000	4204	4242	0040	2240
3 1 1 5 3	1000	4002	4200	2022	4442
3 5 1 5 3	5000	4022	0002	0442	0200
3 3 3 5 3	5000	2240	0040	4242	4204
3 1 5 5 3	5000	0404	0024	2042	2202
3 5 5 5 3	3000	0424	2420	0402	4020
2 2 0 0 4	2000	4404	4024	0042	0202
2 0 2 0 4	2000	2022	4002	4442	4200
2 4 2 0 4	0000	2042	0404	2202	0024

(continued..)

2 0 4 0 4	4000	0220	2244	4422	0440
2 4 4 0 4	2000	0240	4040	2242	2204
2 2 0 2 4	4000	0044	4004	4224	4400
2 0 2 2 4	4000	4202	4042	2024	2404
2 4 2 2 4	2000	4222	0444	0444	4222
2 2 4 2 4	2000	2440	0422	4244	2220
2 0 0 4 4	4000	2244	0440	0220	4422
2 4 0 4 4	2000	2204	2242	4040	0240
2 2 2 4 4	2000	0422	2220	2440	4244
2 0 4 4 4	2000	4040	2204	0240	2242
2 4 4 4 4	0000	4000	4000	4000	4000
3 3 1 1 5	3000	4404	4024	0042	0202
3 1 3 1 5	1000	2022	4002	4442	4200
3 5 3 1 5	5000	2042	0404	2202	0024
3 3 5 1 5	5000	0200	0442	0002	4022
3 1 1 3 5	1000	0004	0400	2044	0224
3 5 1 3 5	5000	0024	2202	0404	2042
3 3 3 3 5	5000	4242	2240	4204	0040
3 1 5 3 5	5000	2400	2224	2004	4044
3 5 5 3 5	3000	2420	4020	0424	0402
3 3 1 5 5	5000	2224	4044	2400	2004
3 1 3 5 5	5000	0442	4022	0200	0002
3 5 3 5 5	3000	0402	0424	4020	2420
3 3 5 5 5	3000	4020	0402	2420	0424
5 5 5 1 3	1000	4004	4400	0044	4224
5 3 1 3 3	3000	4402	4424	2020	0420
5 1 3 3 3	3000	2020	4402	0420	4424
5 5 3 3 3	1000	2040	0204	4240	0242
5 3 5 3 3	1000	0204	0242	2040	4240
5 1 1 5 3	3000	0002	0200	4022	0442
5 5 1 5 3	1000	0022	2002	2442	2200
5 3 3 5 3	1000	4240	2040	0242	0204
5 1 5 5 3	1000	2404	2024	4042	4202
5 5 5 5 3	5000	2424	4420	2402	0020
4 2 0 0 4	4000	0404	0024	2042	2202
4 0 2 0 4	4000	4022	0002	0442	0200
4 4 2 0 4	2000	4042	2404	4202	2024
4 2 4 0 4	2000	2200	2442	2002	0022
4 0 0 2 4	4000	2004	2400	4044	2224
4 4 0 2 4	2000	2024	4202	2404	4042
4 2 2 2 4	2000	0242	4240	0204	2040
4 0 4 2 4	2000	4400	4224	4004	0044
4 4 4 2 4	0000	4420	0020	2424	2402
4 2 0 4 4	2000	4224	0044	4400	4004
4 0 2 4 4	2000	2442	0022	2200	2002
4 4 2 4 4	0000	2402	2424	0020	4420
4 2 4 4 4	0000	0020	2402	4420	2424
5 1 1 1 5	1000	0424	2420	0402	4020
5 5 1 1 5	5000	0444	4222	4222	0444
5 3 3 1 5	5000	4002	4200	2022	4442
5 1 5 1 5	5000	2220	4244	0422	2440

2 2 4 0 4	0000	0200	0442	0002	4022
2 0 0 2 4	2000	0004	0400	2044	0224
2 4 0 2 4	0000	0024	2202	0404	2042
2 2 2 2 4	0000	4242	2240	4204	0040
2 0 4 2 4	0000	2400	2224	2004	4044
2 4 4 2 4	4000	2420	4020	0424	0402
2 2 0 4 4	0000	2224	4044	2400	2004
2 0 2 4 4	0000	0442	4022	0200	0002
2 4 2 4 4	4000	0402	0424	4020	2420
2 2 4 4 4	4000	4020	0402	2420	0424
3 1 1 1 5	5000	4424	0420	4402	2020
3 5 1 1 5	3000	4444	2222	2222	4444
3 3 3 1 5	3000	2002	2200	0022	2442
3 1 5 1 5	3000	0220	2244	4422	0440
3 5 5 1 5	1000	0240	4040	2242	2204
3 3 1 3 5	3000	0044	4004	4224	4400
3 1 3 3 5	3000	4202	4042	2024	2404
3 5 3 3 5	1000	4222	0444	0444	4222
3 3 5 3 5	1000	2440	0422	4244	2220
3 1 1 5 5	3000	2244	0440	0220	4422
3 5 1 5 5	1000	2204	2242	4040	0240
3 3 3 5 5	1000	0422	2220	2440	4244
3 1 5 5 5	1000	4040	2204	0240	2242
3 5 5 5 5	5000	4000	4000	4000	4000
5 1 1 3 3	1000	4422	0220	0440	2244
5 5 1 3 3	5000	4442	2022	4200	4002
5 3 3 3 3	5000	2000	2000	2000	2000
5 1 5 3 3	5000	0224	2044	0400	0004
5 5 5 3 3	3000	0244	4440	4220	2422
5 3 1 5 3	5000	0042	4404	0202	4024
5 1 3 5 3	5000	4200	4442	4002	2022
5 5 3 5 3	3000	4220	0244	2422	4440
5 3 5 5 3	3000	2444	0222	0222	2444
4 0 0 0 4	2000	0424	2420	0402	4020
4 4 0 0 4	0000	0444	4222	4222	0444
4 2 2 0 4	0000	4002	4200	2022	4442
4 0 4 0 4	0000	2220	4244	0422	2440
4 4 4 0 4	4000	2240	0040	4242	4204
4 2 0 2 4	0000	2044	0004	0224	0400
4 0 2 2 4	0000	0202	0042	4024	4404
4 4 2 2 4	4000	0222	2444	2444	0222
4 2 4 2 4	4000	4440	2422	0244	4220
4 0 0 4 4	0000	4244	2440	2220	0422
4 4 0 4 4	4000	4204	4242	0040	2240
4 2 2 4 4	4000	2422	4220	4440	0244
4 0 4 4 4	4000	0040	4204	2240	4242
4 4 4 4 4	2000	0000	0000	0000	0000
5 3 1 1 5	3000	0404	0024	2042	2202
5 1 3 1 5	3000	4022	0002	0442	0200
5 5 3 1 5	1000	4042	2404	4202	2024
5 3 5 1 5	1000	2200	2442	2002	0022

(continued..)

5 5 5 1 5	3000	2240	0040	4242	4204
5 3 1 3 5	5000	2044	0004	0224	0400
5 1 3 3 5	5000	0202	0042	4024	4404
5 5 3 3 5	3000	0222	2444	2444	0222
5 3 5 3 5	3000	4440	2422	0244	4220
5 1 1 5 5	5000	4244	2440	2220	0422
5 5 1 5 5	3000	4204	4242	0040	2240
5 3 3 5 5	3000	2422	4220	4440	0244
5 1 5 5 5	3000	0040	4204	2240	4242
5 5 5 5 5	1000	0000	0000	0000	0000
1 3 1 3 3	5000	0402	0424	4020	2420
1 1 3 3 3	5000	4020	0402	2420	0424
1 5 3 3 3	3000	4040	2204	0240	2242
1 3 5 3 3	3000	2204	2242	4040	0240
1 1 1 5 3	1000	2002	2200	0022	2442
1 5 1 5 3	3000	2022	4002	4442	4200
1 3 3 5 3	3000	0240	4040	2242	2204
1 1 5 5 3	3000	4404	4024	0042	0202
1 5 5 5 3	1000	4424	0420	4402	2020
0 2 0 0 4	0000	2404	2024	4042	4202
0 0 2 0 4	0000	0022	2002	2442	2200
0 4 2 0 4	4000	0042	4404	0202	4024
0 2 4 0 4	4000	4200	4442	4002	2022
0 0 0 2 4	0000	4004	4400	0044	4224
0 4 0 2 4	4000	4024	0202	4404	0042
0 2 2 2 4	4000	2242	0240	2204	4040
0 0 4 2 4	4000	0400	0224	0004	2044
0 4 4 2 4	2000	0420	2020	4424	4402
0 2 0 4 4	4000	0224	2044	0400	0004
0 0 2 4 4	4000	4442	2022	4200	4002
0 4 2 4 4	2000	4402	4424	2020	0420
0 2 4 4 4	2000	2020	4402	0420	4424
1 1 1 1 5	3000	2424	4420	2402	0020
1 5 1 1 5	1000	2444	0222	0222	2444
1 3 3 1 5	1000	0002	0200	4022	0442
1 1 5 1 5	1000	4220	0244	2422	4440
1 5 5 1 5	5000	4240	2040	0242	0204
1 3 1 3 5	1000	4044	2004	2224	2400
1 1 3 3 5	1000	2202	2042	0024	0404
1 5 3 3 5	5000	2222	4444	4444	2222
1 3 5 3 5	5000	0440	4422	2244	0220
1 1 1 5 5	1000	0244	4440	4220	2422
1 5 1 5 5	5000	0204	0242	2040	4240
1 3 3 5 5	5000	4422	0220	0440	2244
1 1 5 5 5	5000	2040	0204	4240	0242
1 5 5 5 5	3000	2000	2000	2000	2000

5 1 1 3 5	3000	2004	2400	4044	2224
5 5 1 3 5	1000	2024	4202	2404	4042
5 3 3 3 5	1000	0242	4240	0204	2040
5 1 5 3 5	1000	4400	4224	4004	0044
5 5 5 3 5	5000	4420	0020	2424	2402
5 3 1 5 5	1000	4224	0044	4400	4004
5 1 3 5 5	1000	2442	0022	2200	2002
5 5 3 5 5	5000	2402	2424	0020	4420
5 3 5 5 5	5000	0020	2402	4420	2424
1 1 1 3 3	3000	0422	2220	2440	4244
1 5 1 3 3	1000	0442	4022	0200	0002
1 3 3 3 3	1000	4000	4000	4000	4000
1 1 5 3 3	1000	2224	4044	2400	2004
1 5 5 3 3	5000	2244	0440	0220	4422
1 3 1 5 3	1000	2042	0404	2202	0024
1 1 3 5 3	1000	0200	0442	0002	4022
1 5 3 5 3	5000	0220	2244	4422	0440
1 3 5 5 3	5000	4444	2222	2222	4444
0 0 0 0 4	4000	2424	4420	2402	0020
0 4 0 0 4	2000	2444	0222	0222	2444
0 2 2 0 4	2000	0002	0200	4022	0442
0 0 4 0 4	2000	4220	0244	2422	4440
0 4 4 0 4	0000	4240	2040	0242	0204
0 2 0 2 4	2000	4044	2004	2224	2400
0 0 2 2 4	2000	2202	2042	0024	0404
0 4 2 2 4	0000	2222	4444	4444	2222
0 2 4 2 4	0000	0440	4422	2244	0220
0 0 0 4 4	2000	0244	4440	4220	2422
0 4 0 4 4	0000	0204	0242	2040	4240
0 2 2 4 4	0000	4422	0220	0440	2244
0 0 4 4 4	0000	2040	0204	4240	0242
0 4 4 4 4	4000	2000	2000	2000	2000
1 3 1 1 5	5000	2404	2024	4042	4202
1 1 3 1 5	5000	0022	2002	2442	2200
1 5 3 1 5	3000	0042	4404	0202	4024
1 3 5 1 5	3000	4200	4442	4002	2022
1 1 1 3 5	5000	4004	4400	0044	4224
1 5 1 3 5	3000	4024	0202	4404	0042
1 3 3 3 5	3000	2242	0240	2204	4040
1 1 5 3 5	3000	0400	0224	0004	2044
1 5 5 3 5	1000	0420	2020	4424	4402
1 3 1 5 5	5000	0224	2044	0400	0004
1 1 3 5 5	3000	4442	2022	4200	4002
1 5 3 5 5	1000	4402	4424	2020	0420
1 3 5 5 5	1000	2020	4402	0420	4424
0 0 0 0 0	0000	0000	0000	0000	0000

REFERENCES

[1] E. R. Berlekamp, Algebraic Coding Theory, McGraw-Hill, New York, 1968.

[2] W. W. Peterson and E. J. Weldon, Jr., Error Correcting codes, 2nd Edition, Cambridge, M.I.T., 1972.

[3] I. F. Blake and R. C. Mullin, Mathematical Theory of Coding, Academic Press, New York, 1975.

[4] Vera Pless, Introduction to the theory of Error Correcting Codes, John Wiley and Sons, 1982.

[5] Shu Lin, An Introduction to Error Correcting Codes, Prentice Hall, 1970.

[6] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error Correcting Codes, North Holland Publishing Company, New York, 1981.

[7] Jessie MacWilliams, "Error correcting codes for Multi-level transmission", Bell System Technical Journal, Jan.1961, pp.281-308.

[8] I. F. Blake, "Codes over certain rings", Inform. Control, vol.20, pp.396-404, 1972.

[9] I. F. Blake, "Codes over integer residue rings", Inform. Control, vol.29, pp.295-300, 1975.

[10] E. Spiegel, "Codes over Z_m", Inform. Control, vol.35, pp.48-52, 1977.

[11] E. Spiegel, "Codes over Z_m-Revisited", Inform. Control, vol.37, pp.100-104, 1978.

[12] Prithi Shankar, "On BCH codes over arbitrary integer rings", IEEE Trans. Inform. Theory, vol.IT-25, No.4, pp.480-483, July 1979.

[13] S. K. Wasan, "On Codes over Z_m", IEEE Trans. Inform. Theory, vol.IT-28, No.1, Jan.1982, pp.117-120.

[14] R. E. Blahut, "Algebraic codes in the frequency domain", CISM Courses and lectures, No.258, Springer-Verlag, New York.

[15] R. E. Blahut, Theory and Practice of Error Control Codes, Addision-Wesley, California 1983.

[16] H. F. Mattson, Jr. and G. Solomon, "A New Treatment of Bose-Chaudhuri Codes", J. Soc. Indust. Appl. Math., vol.9, 1961, pp.654-669.

[17] R. C. Agarwal and C. S. Burrus, "Fast convolution using Fermat number transforms with applications in digital filtering", IEEE Trans. Acoust. Speech Signal Processing, vol.ASSP-22, pp.87-97, 1974.

[18] P. J. Nicholson, "Algebraic theory of finite Fourier transforms", J. Comput. Syst. Sys., vol.5, pp.524-547, 1971.

[19] I. S. Reed and T. K. Truong, "Complex integer convolutions over a direct sum of Galois fields", IEEE Trans. Inform. Theory, vol.IT-21, No.26, pp.657-661, 1975.

[20] -------, "Convolutions over residue classes of quadratic integers", IEEE Trans. Inform Theory, vol.IT-22, No.4, pp.468-475, 1976.

[21] E. Dubois and A. N. Venetsanopoulos, "Convolution using a conjugate symmetry property for the generalized discrete Fourier transform", IEEE Trans. Acoust. Speech Signal Processing, vol.ASSP-26, pp.165-169, 1978.

[22] ------, "The discrete Fourier transform over finite rings with application to fast convolution", IEEE Trans. Computers, vol.C-27, pp.586-593, 1978.

[23] J. B. Martens and M. C. Vanwormhoudt, "Convolution using a conjugate symmetry property for number theoretic transforms over rings of regular integers", IEEE Trans. ASSP, vol.ASSP-31, No.5, 1983, pp.1121-1124.

[24] B. R. McDonald, Finite Rings with Identity, Marcel-Decker, New York, 1974.

[25] R. Raghavendran, "Finite associative rings", Compositio Mathematica, vol.21, pp.195-229, 1969.

[26] H. S. Madhusudhana, On abelian codes which are closed under cyclic shifts, M.Tech Thesis, Indian Institute of Tech., Kanpur (India), 1987.

[27] F. J. MacWilliams, 'Binary codes which are ideals in the group algebra of an abelian group' BSTJ, No.49, (July-Augest 1970), pp.987-1011.

[28] Paulo Ribenboim, Rings and modules, Interscience Tracts in Pure and Applied Mathematics, Interscience Publishers, New York.

[29] J. Chiang and J. K. Wolf, "On channels and codes for the Lee metric", Inform. Control, vol.19, pp.159-173, 1971.

[30] D. J. Britten and E. W. Lemire, "A structure theorem for rings supporting a discrete Fourier transform", SIAM J. Applied Maths., vol.41, pp.222-226, Oct 1981.

[31] H. Murakami, I. S. Reed and L. R. Welch, "A transform decoder for Reed-Solomon codes in multiple user communication systems", IEEE Trans. Inform. Theory, vol.IT-23, No.1977, pp.1745-1753.

[32] P. Camion, 'Abelian codes', Math. Research Center, Univ. of Wisconsin, Report No.1059, 1970.

[33] S. D. Berman, 'Semi-simple cyclic and Abelian codes', Kibernetica, vol.3, No.3, 1967, pp.21-30.

[34] S. D. Berman, "On the theory of Group Codes", Kibernetika, vol.3, No.1, pp.31-39, 1967.

[35] P. Delsarte, 'Automorphisms of Abelian codes', Philips Research Repts. 25, 1970, pp.389-403.

[36] R. J. Miller, 'Minimal codes in Abelian group algebras', J. Combinatorial Theory, Series A26 (1979), pp.166-178.

[37] B. Sundar Rajan, Spectral characterisation of Abelian group codes, M.Tech thesis, I.I.T. Kanpur, India, 1984.

[38] H. O. Burton, and E. J. Weldon, Jr., "Cyclic Product Codes", IEEE Trans. Inform. Theory, vol.IT-11, 1965, pp.433-439.

[39] N. S. Szabo and R. I. Tanaka, Residue arithmetic and its applications to Computer Technology, McGraw Hill, New York, 1967.

[40] M. U. Siddiqi, A study of permutation invariant linear systems, Ph.D thesis, I.I.T. Kanpur, India, 1976.

[41] P. Delsarte, "Bounds for unrestricted codes by linear programming", Philips Research Deve.J., vol.27, pp.272-289, 1972.

[42] M. Hall, Jr., The Theory of Groups, MacMillan, 1964.

[43] J. L. Massey, "Shift register synthesis and BCH decoding" IEEE Trans.Inform.Theory, vol.IT-16, No.1, Jan.1969, pp.122-127.

[44] J. A. Reeds and N. J. A. Sloane, "Shift register synthesis (modulo m)," SIAM J. Computing, Aug.1985, pp.505-513.

[45] E. E. Nemirovskiy, "Codes on residue class rings with multi-frequency phase telegraphy", Radiotechnika i electronika, No.9, 1984, pp.1745-1753.

EE-1989-D-RAJ-TRA.